Wireless G 2.4GHz 500mW Outdoor AP

Model: APO1000/APO1010

User's Manual

V.1.0

Table of Contents

Chapter 1. System Overview

1.1 Introduction

The 802.11 b/g compliant Airlink101® APO1000/APO1010 is an outdoor wireless access point that can be used for five different purposes in three different modes. In the AP mode, it can be deployed either as traditional fixed wireless Access Point(AP), or combination of AP and WDS(AP+WDS). In the WDS mode, it's only used to expand or bridge Ethernet networks and deployed as a main base, relay based or remote base station. In the CPE (Customer Premises Equipment) mode, it connects to Wireless Internet Service Provider's (WISP) outdoor network via wireless WAN gateway to access to Internet. In the Client Bridge + Universal Repeater mode, it connects to Wireless Internet Service Provider's (WISP) outdoor network via wireless or wired bridge to access to Internet

The die-cast sealed APO1000/APO1010 is compact in size and compliant with IP68 weatherproof standard. It comes with a mounting kit to mount on pole or wall. It is suitable for both indoor and outdoor usage with its 500mW output power, which is higher than a typical indoor AP (100mW).

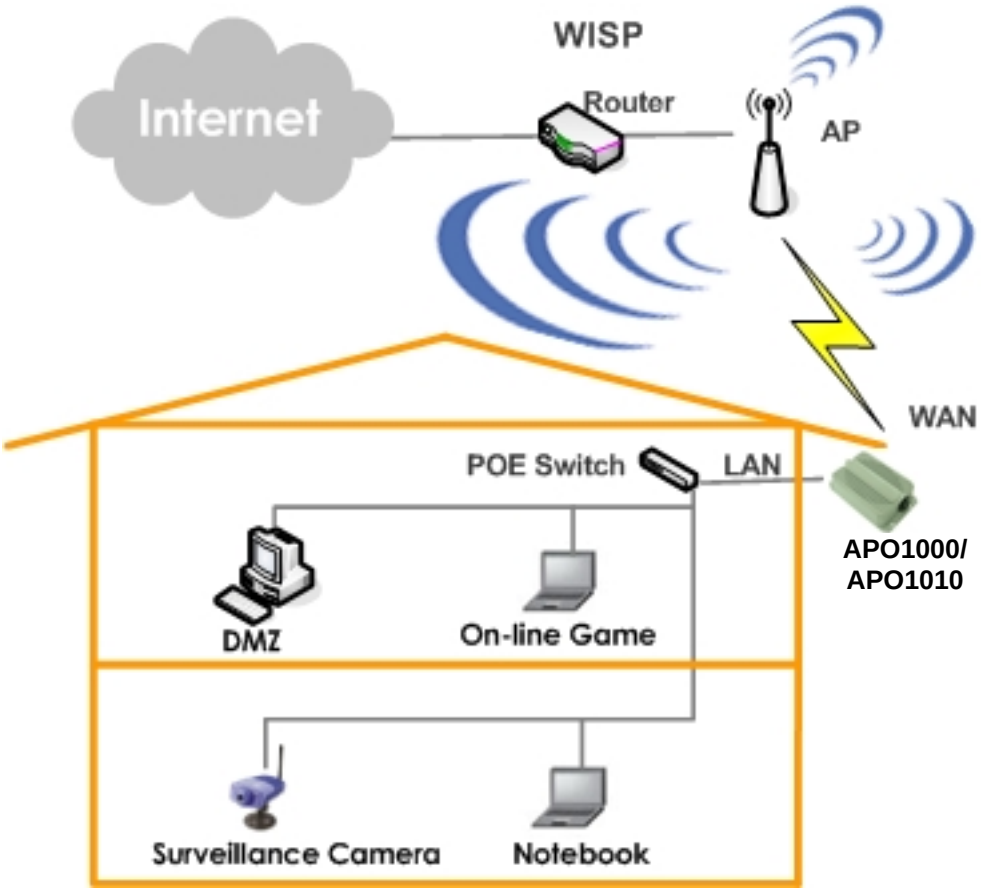
Features:

1. Access Point : It can be deployed as a traditional fixed wireless Access Point
2. Repeater: To expand wireless service by repeating prior AP
3. WDS : It can be used to expand Ethernet network via wireless WDS Link
4. AP+WDS: Not only to extend Ethernet network, but also provide wireless access to the expanded network
5. CPE (Customer Premises Equipment): It is a wireless gateway with NAT and DHCP Server functions to connects to Wireless Internet Service Provider's (WISP)
6. Client Bridge + Universal Repeater : It is a wireless repeater or bridge to connects to Wireless Internet Service Provider's (WISP)

1.2 System Concept

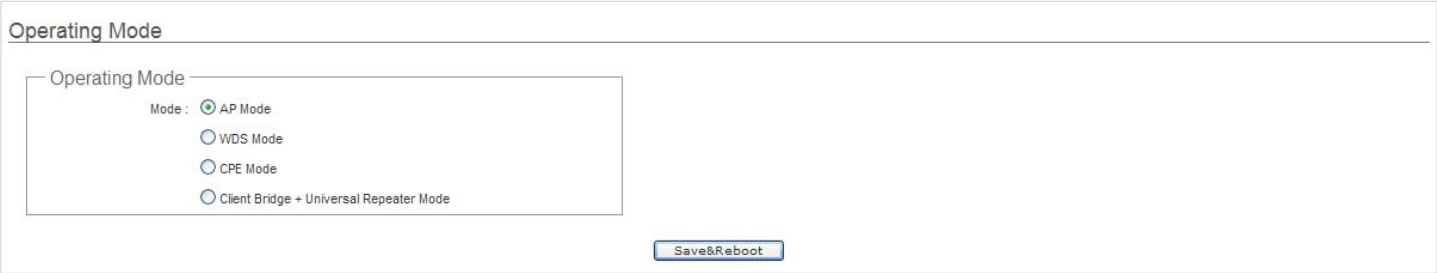
The APO1000/APO1010 is not only designed and used as traditional outdoor AP, but also with rich features tailored for WISP applications. The two-level management capability and access control ease WISP and owners to maintain and manage wireless network in a more controllable fashion. Main applications are listed as follows with illustration:

1. Wireless CPE for Multi Dwelling Unit/Multi Tenant Unit (MDU/MTU) complexes including apartments, dormitories, and office complexes.
2. Outdoor Access Point for school campuses, enterprise campuses, or manufacture plants.
3. Indoor Access Point for hotels, factories, or warehouses where industrial grade devices are preferred.
4. Public hotspot operation for café, parks, convention centers, shopping malls, or airports.
5. Wireless coverage for indoor and outdoor grounds in private resorts, home yards, or gulf course communities.



1.3 Applications in Wireless Network

APO1000/APO1010 is a multiple mode system which can be configured either as a wireless gateway or an access point as desired. It also can be used as WDS link for Ethernet network expansion. This section depicts different applications in **AP Mode**, **WDS Mode**, and **CPE Mode** and **Client Bridge + Universal Repeater Mode**.



■ Configuration in AP Mode (including Access Point + WDS)

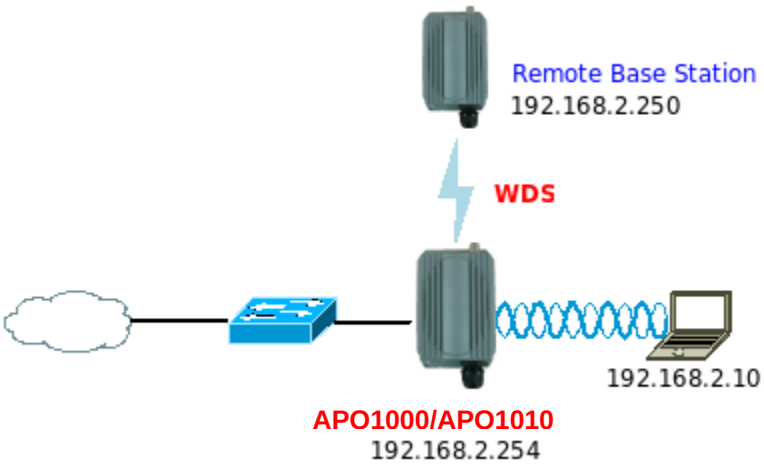
An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly.

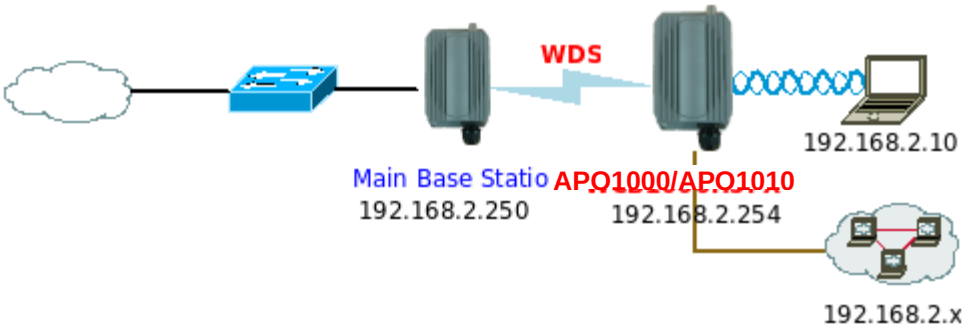
➔ **Example 1 :** Access Point without WDS

✓ It can be deployed as a tradition fixed wireless Access Point

➔ **Example 2 :** Access Point with WDS

✓ It can be deployed as a tradition fixed wireless Access Point and provides WDS link to expand network

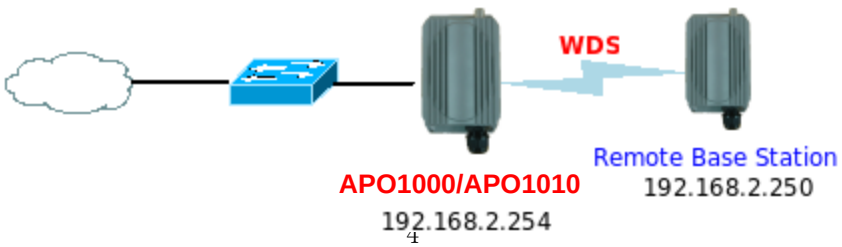


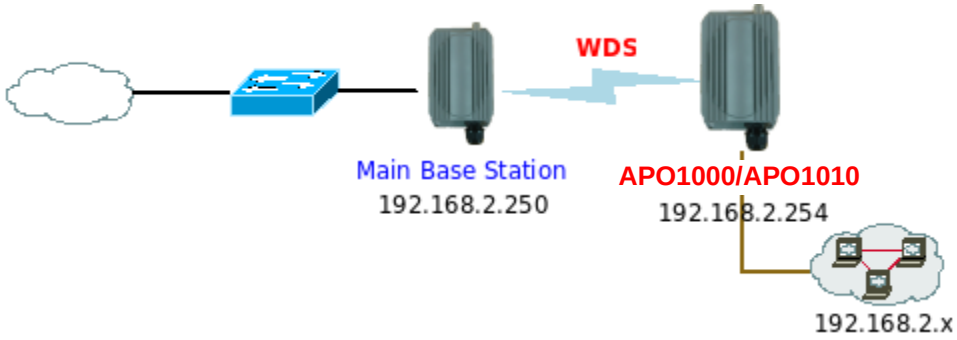


- **Configuration in WDS Mode (Pure WDS)**

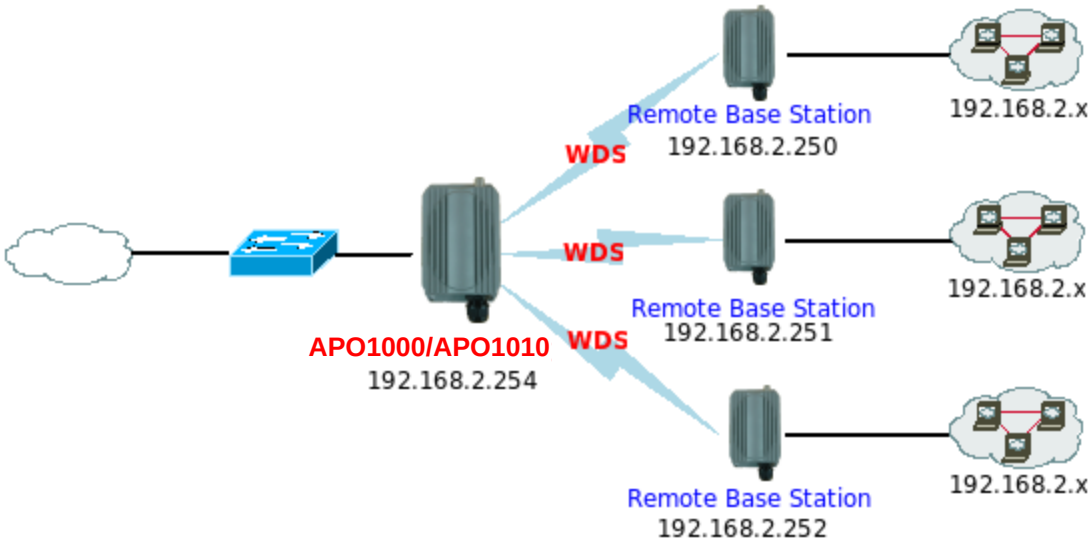
  An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly. In this mode, it can support single or multiple WDS links and no wireless clients **can** associate with it though.

  ➔ **Example 1 :** Point-to-Point

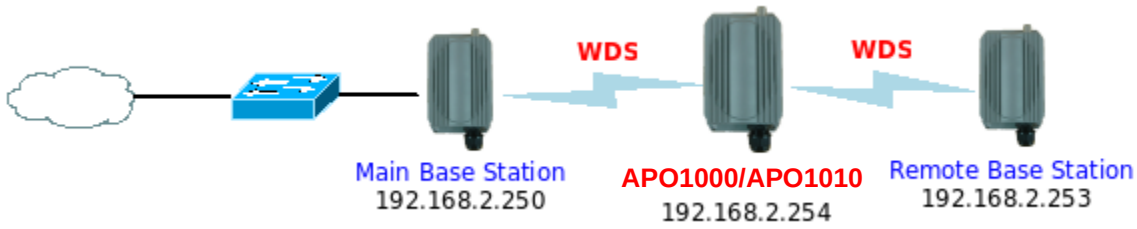



WDS
Main Base Station
192.168.2.250
APO1000/APO1010
192.168.2.254
192.168.2.x

➔ **Example 2 :** Point-to-Multi-Point

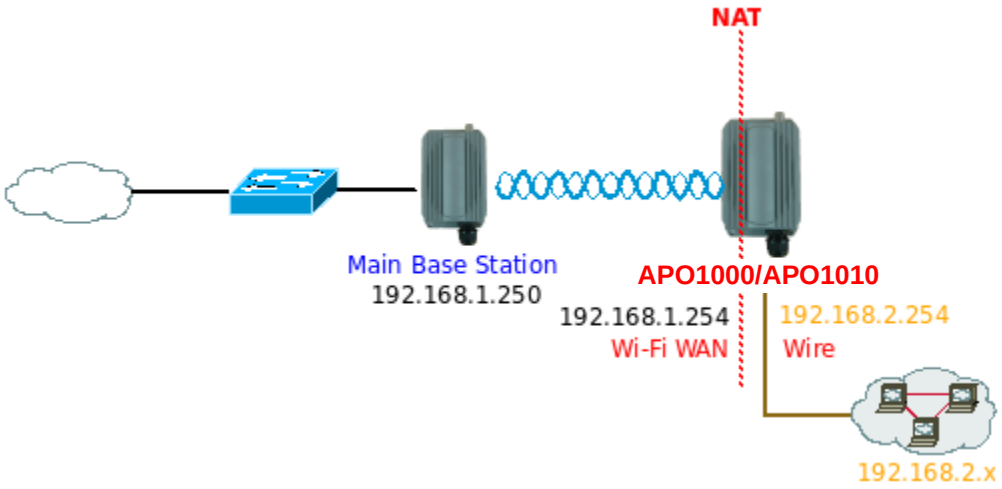


➔ **Example 3 :** Multi-Point Repeating bridge



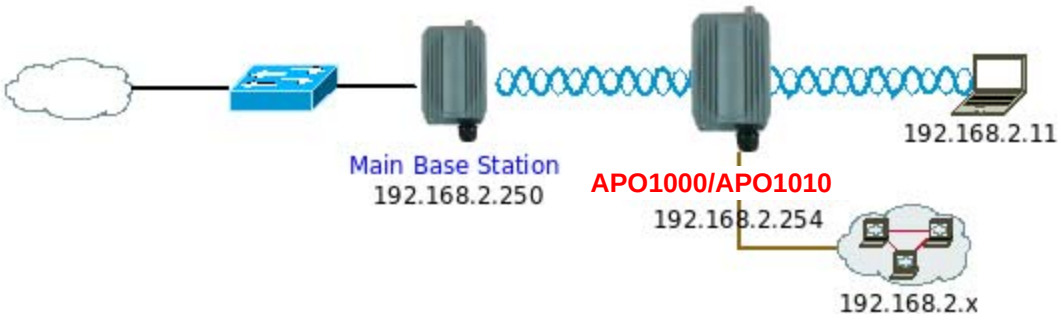
■ Configuration in CPE Mode

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE mode, APO1000/APO1010 is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to APO1000/APO1010 are in **different** subnet from those connected to Main Base Station, and, in CPE mode, it **does not** accept wireless association from wireless clients.



■ Configuration in Client Bridge + Universal Repeater Mode

It can be used as an Client Bridge + Universal Repeater to receive wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, APO1000/APO1010 is enabled with DHCP Server functions. The wired clients of APO1000/APO1010 are in **the same** subnet from Main Base Station and it **accepts** wireless connections from client devices.



1.4 Product Benefit

- 500mW at 2.4Ghz Output Power
- Topology : Point to Point ; Point to Multi Point
- Operation Modes :
  - ➔ Access Point Mode : Pure Access Point Function and Access Point /Bridge(WDS) Function
  - ➔ WDS Mode
  - ➔ CPE Mode (Router Client)
  - ➔ Client Bridge + Universal Repeater Mode
- Security with WEP, WPA/WPA2-PSK, and WPA/WPA2-RADIUS
- Over load current protection
- Integrated Power over Ethernet (PoE)
- 8 Multiple B-SSID capability
- Business-class security and central management
- Weather-Proof Housing
- VLAN tag over WDS
- Client Isolation through Layer 2 VLAN technology
- Two administrator accounts for manager authorities

APO1000/APO1010 outdoor high power WiFi Bridge is the point of connection to Wireless Outdoor Network for service provider deploying last mile services to business or residential broadband subscribers.. Network administrators can create multiple subscriber service tier using per-subscriber rate limiting features, and manage centrally. APO1000/APO1010 outdoor bridge utilizes a 500mW output Tx Power to connect to the WiFi mesh or WDS infrastructure and provides the subscriber with an Ethernet connection for a local access.

APO1000/APO1010 outdoor high power Bridge supports four operational modes, the AP mode, the WDS mode, the CPE mode and the Client Bridge + Universal Repeater mode, respectively with built-in remote management features.

1.5 Specification

- **Wireless Architecture Mode**
  - ➔ **AP Mode**
    - ✓ **Pure AP Mode**
      - It can be deployed as a tradition fixed wireless Access Point
      - It allow wireless clients or Stations(STA) to access
    - ✓ **AP/WDS Mode**
      - This enables the wireless interconnection of Access Point in an IEEE802.11 network .and accept wireless clients at the same time
  - ➔ **WDS Mode**
    - ✓ This enables the wireless interconnection of Access Point in an IEEE802.11 network.
    - ✓ It allows a wireless network to be expanded using multiple access point without the need for a wired backbone to link them.
    - ✓ This also be referred to as repeater mode.
    - ✓ It can't allow wireless clients or Stations (STA) to associate.
  - ➔ **CPE Mode**
    - ✓ WiFi connection as WAN , in CPE mode , the device run as DHCP server to assign IP address to clients out of a private IP address pool behind a NAT
  - ➔ **Client Bridge + Universal RepeaterMode**
    - ✓ A wireless repeater and bridge with DHCP server enabled, clients on the same subnet as host AP(Primary Router).

6. Networking

- ➔ Support Static IP, Dynamic IP(DHCP Client) and PPPoE on WiFi WAN Connection
- ➔ Support PPTP/L2TP/IP Sec Pass Through
- ➔ PPPoE Reconnect – Always On , On demand, Manual
- ➔ MAC Cloning
- ➔ DHCP Server
- ➔ 802.3 Bridging
- ➔ Masquerading (NAT)
- ➔ Proxy DNS
- ➔ Dynamic DNS
- ➔ NTP Client
- ➔ Virtual DMZ
- ➔ Virtual Server (IP / Port Forwarding)

- ➔ Support MAC Filter
- ➔ Support IP Filter
- ➔ Bandwidth traffic Shaping

7. Wireless Feature

- ➔ Transmission power control : 9 Levels
- ➔ Channel selection : Manual or Auto
- ➔ No of associated clients per AP : 32
- ➔ Setting for max no associated clients : Yes
- ➔ No. of ESSID (Virtual AP) : 8
- ➔ No. of Max. WDS setting : 8
- ➔ Preamble setting : Short/ Long
- ➔ Setting for 802.11b/g mix, 802.11b only or 802.11g only
- ➔ Setting for transmission speed
- ➔ Dynamic Wireless re-transmission
- ➔ IEEE802.11f IAPP (Inter Access Point Protocol), hand over users to another AP
- ➔ IEEE 802.11i Preauth (PMKSA Cache)
- ➔ IEEE 802.11h -Transmission Power Control
- ➔ IEEE 802.11d -Multi country roaming

■ **Authentication/ Encryption (Wireless Security)**

- ➔ Layer 2 User Isolation
- ➔ Blocks client to client discovery within a specified VLAN
- ➔ WEP 64/ 128/ 152 Bits
- ➔ EAP-TLS + Dynamic WEP
- ➔ EAP-TTLS + Dynamic WEP
- ➔ PEAP/ MS-PEAP+Dynamic WEP
- ➔ WPA (PSK +TKIP)
- ➔ WPA (802.1x certification + TKIP)
- ➔ 802.11i WPA2 (PSK + CCMP/ AES)
- ➔ 802.11i WPA2 (802.1x certification + CCMP/ AES)
- ➔ Setting for TKIP/ CCMP/ AES key's refreshing period
- ➔ Hidden ESSID support
- ➔ Setting for "Deny ANY " connection request
- ➔ MAC Address filtering (MAC ACL)

- ➔ No. of registered RADIUS servers : 2
- ➔ VLAN assignment on BSSID
- ➔ Support VLAN tag over WDS

- **Quality of Service**
  - ➔ DiffServ/ ToS
  - ➔ IEEE802.1p/ CoS
  - ➔ IEEE 802.1Q Tag VLAN priority control
  - ➔ IEEE802.11e WMM

- **System Administration**
  - ➔ Intuitive Web Management Interface
  - ➔ Password Protected Access
  - ➔ Firmware upgrade via Web
  - ➔ Reset to Factory Defaults
  - ➔ Profiles Configuration Backup and Restore
  - ➔ Two administrator accounts
  - ➔ Remote Link Test
  - ➔ Full Statistics and Status Reporting
  - ➔ SNMP Traps to a list of IP Address
  - ➔ NTP Time Synchronization
  - ➔ Even Log
  - ➔ Support SNMP v1,v2c, v3
  - ➔ Support MIB II
  - ➔ CLI access via Telnet and SSH
  - ➔ Administrative Access : HTTP/ HTTPS
  - ➔ UPnP (Universal Plug and Play)

Chapter 2. Basic Installation

2.1 Hardware Installation

2.1.1 Package Contents

The standard package contents of APO1000/APO1010:

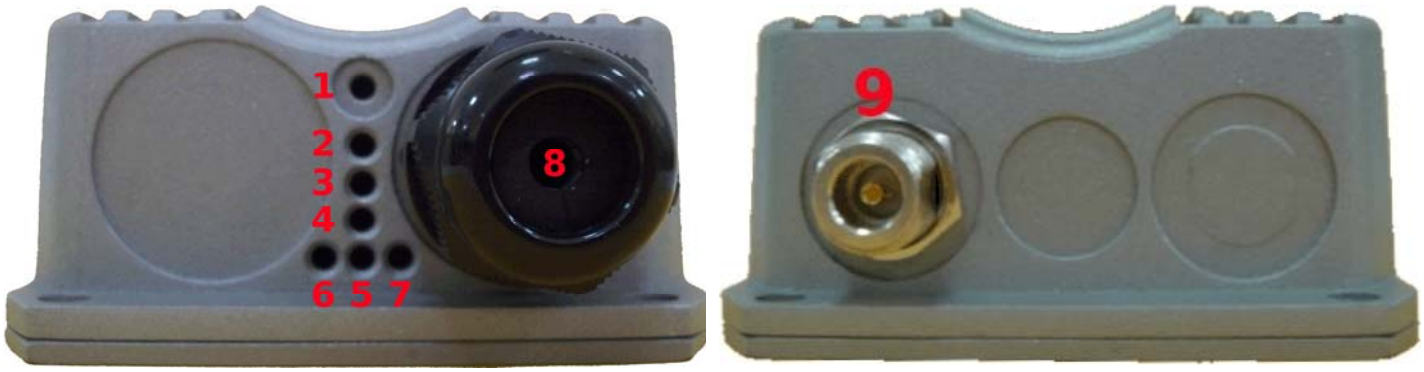
- APO1000/APO1010 x 1
- Quick Installation Guide x 1
- CD-ROM (with User Manual and QIG) x 1
- PSE with AC Cable x 1
- Mounting Kit x 1

It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

2.1.2 Panel Function Descriptions

- **APO1000**

Front Panel **Rear Panel**



1. Reset Button : System reboot button press until LED flashed and release for system reboot or for reset to factory default press, LED flashes keep pressing until LED becomes static
2. Power : Red LED ON indicates power on, and OFF indicates power off
3. Signal Strength : Yellow LED ON indicates Low Signal (CPE Mode)
4. Signal Strength : Green LED ON indicates Normal Signal (CPE Mode) or (WDS Mode only)
5. Signal Strength : Green LED ON indicates High Signal (CPE Mode) or (AP Mode only)
6. WLAN : Green LED BLINKING indicates Wireless ON, and BLINKING quickly indicates Wireless Transmit quickly.
7. Ethernet : Green LED ON indicates connection, OFF indicates no connection
8. PoE Connector : For connecting to PSE
9. N-Type Connector : For connecting to N-Type antenna

In CPE Mode, the LED 3 ON indicates the signal Low (Signal <= 10 RSSI); the LED 3 and 4 ON indicate the signal Normal (10 < Signal <=40 RSSI); the LED 3, 4 and 5 ON indicate the signal High (Signal > 40).
Only LED 4 ON indicates the operating mode is WDS Mode; only LED 5 ON indicates the operating mode is AP Mode.

➢ APO1010

Front Panel **Rear Panel**

1. Reset Button : System reboot button press until LED flashed and release for system reboot or for reset to factory default press, LED flashes keep pressing until LED becomes static
2. Power : Red LED ON indicates power on, and OFF indicates power off
3. Signal Strength : Yellow LED ON indicates Low Signal (CPE Mode)
4. Signal Strength : Green LED ON indicates Normal Signal (CPE Mode) or (WDS Mode only)
5. Signal Strength : Green LED ON indicates High Signal (CPE Mode) or (AP Mode only)
6. WLAN : Green LED BLINKING indicates Wireless ON, and BLINKING quickly indicates Wireless Transmit quickly.
7. Ethernet : Green LED ON indicates connection, OFF indicates no connection
8. PoE Connector : For connecting to PSE

In CPE Mode, the LED 3 ON indicates the signal Low (Signal <= 10 RSSI); the LED 3 and 4 ON indicate the signal Normal (10 < Signal <=40 RSSI); the LED 3, 4 and 5 ON indicate the signal High (Signal > 40).
Only LED 4 ON indicates the operating mode is WDS Mode; only LED 5 ON indicates the operating mode is AP Mode.

2.1.3 Hardware Installation Steps

Please follow the steps mentioned below to install the hardware of APO1000/APO1010:

- **APO1000**

Front Panel

Rear Panel

➔ Connect N-type antenna to the N-type connector on the rear panel.

➔ Connect Power Injector to the PoE connector on the front panel.

➔ Connect an Ethernet cable to the Power Injector and the other end to a computer.

➔ Source power to Power Injector in order to supply power to APO1000.

- **APO1010**

Front Panel

Rear Panel

➔ Connect Power Injector to the PoE connector on the front panel.

➔ Connect an Ethernet cable to the Power Injector and the other end to a computer.

➔ Source power to Power Injector in order to supply power to APO1010.

2.2 Web Management Interface Instructions

APO1000/APO1010 supports web-based configuration. Upon the completion of hardware installation, APO1000/APO1010 can be configured through a COMPUTER by using its web browser such as Internet Explorer or Mozilla Firefox.

1. **Default IP Address :** 192.168.2.254
2. **Default IP Netmask :** 255.255.255.0
3. **Default User Name and Password :**

   The default user name and password for both root manager account and admin manager account are as follows:

Mode	**CPE Mode**		**AP Mode**	**WDS Mode**	**Client Bridge + Universal Repeater Mode**
Management Account	Root Account	Admin Account	Root Account	Root Account	Root Account
User Name	root	admin	root	root	root
Password	default	admin	default	default	default

Step

- **IP Segment Set-up for Administrator's Computer**

  Set the IP segment of the administrator's computer to be in the same range as APO1000/APO1010 for accessing the system. Do not duplicate the IP Address used here with IP Address of APO1000/APO1010 or any other device within the network

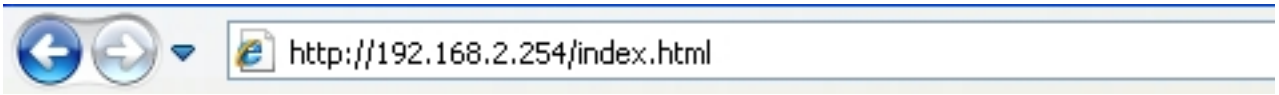
  Example of Segment :

  The valid range is 1 ~ 254 and 192.168.2.254 shall be avoided because it is already assigned to APO1000/APO1010. 192.168.2.10 is used in the example below.

  - ➔ IP Address : 192.168.2.10
  - ➔ IP Netmask : 255.255.255.0

- **Launch Web Browser**

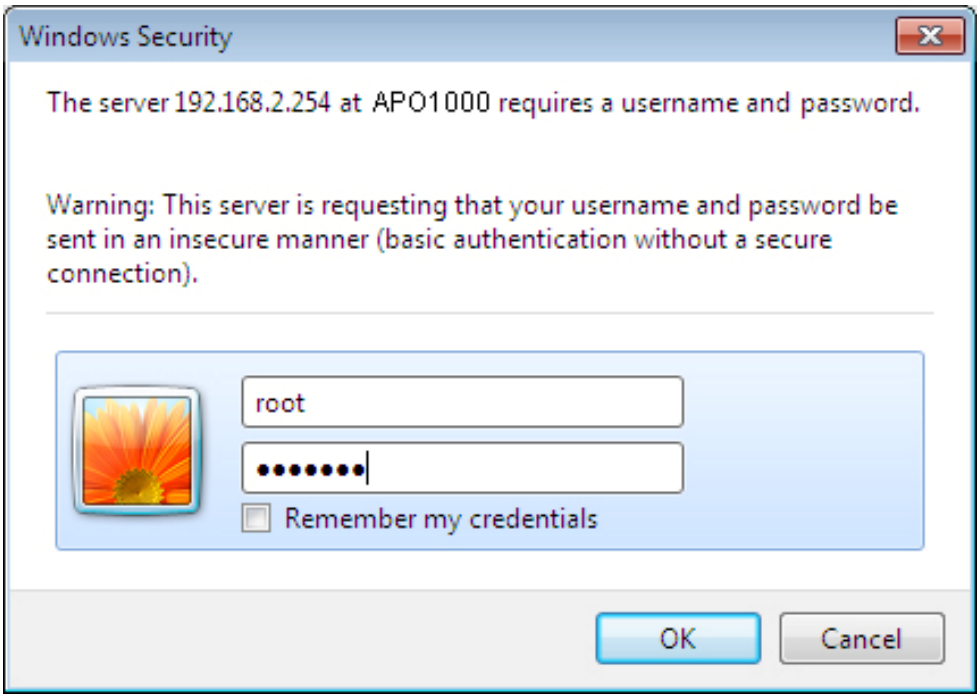
  Launch web browser to access the web management interface of system by entering the default IP Address, http://192.168.2.254, in the URL field, and then press ***Enter***.



System Login

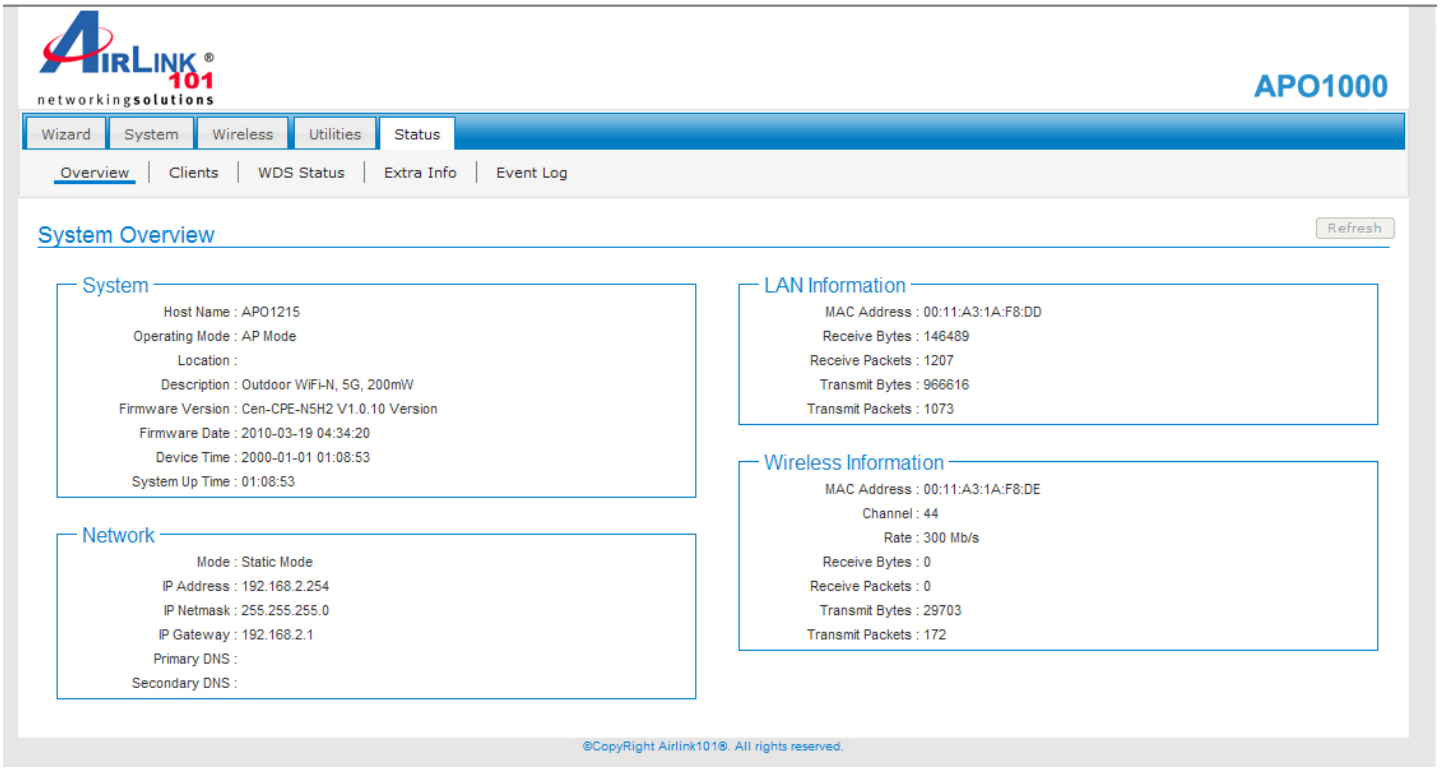
The network manager Login Page then appears.

Enter "***root***" for user name and "**default**" for password, and then click OK to login to the system; the root manager account is used as an example here.



- **Login Success**

System Overview page will appear after successful login.



Chapter 3. AP Mode Configuration

When AP mode is chosen, the system can be configured as an Access Point. This section provides detailed explanation for users to configure in the AP mode with help of illustrations. In the AP mode, functions listed in the table below are also available from the Web-based GUI interface.

Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Settings	Profiles Settings	System Overview
	LAN	Advanced Settings	Firmware Upgrade	Clients
	Management	Virtual AP	Network Utility	WDS List
	Time Server	WDS Setup	Reboot	Extra Info
	SNMP			Event Log
	UPNP			

Table 3-1: AP Mode Functions

3.1 External Network Connection

3.1.1 Network Requirement

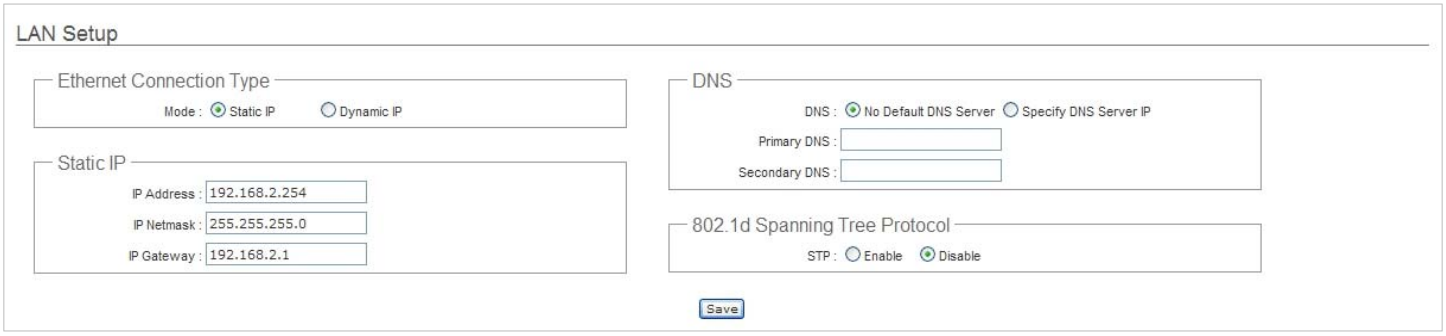
Normally, APO1000/APO1010 connects to a wired LAN and provides a wireless connection point to associate with wireless client as shown in Figure 3-1. Then, Wireless clients could access to LAN or Internet by associating themselves with APO1000/APO1010 set in AP mode.

Figure 3-1 Access Point on a Wired LAN Configuration

3.1.2 Configure LAN IP

Here are the instructions to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.



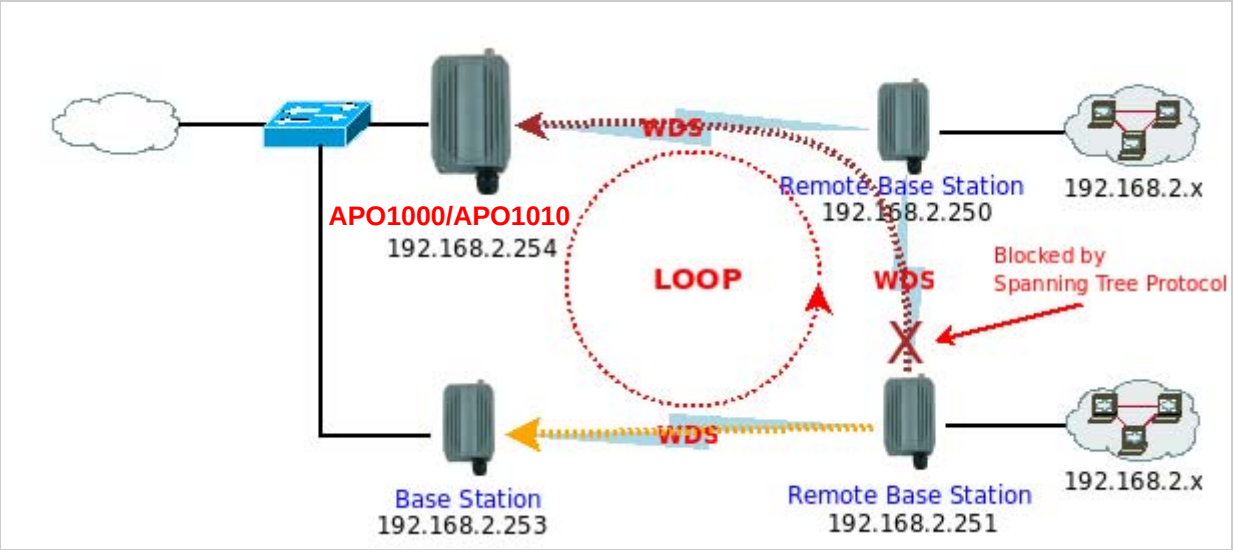
- **Mode :** Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
  - ➔ **Static IP :** The administrator can manually setup the LAN IP address when static IP is preferred.
    - ✓ **IP Address :** The IP address of the LAN port; default IP address is 192.168.1.254
    - ✓ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
    - ✓ **IP Gateway :** The default gateway of the LAN port; default Gateway is 192.168.1.1
  - ➔ **Dynamic IP :** This configuration type is applicable when the APO1000/APO1010 is connected to a network with presence of a DHCP server. All related IP information will be provided by the DHCP server automatically.

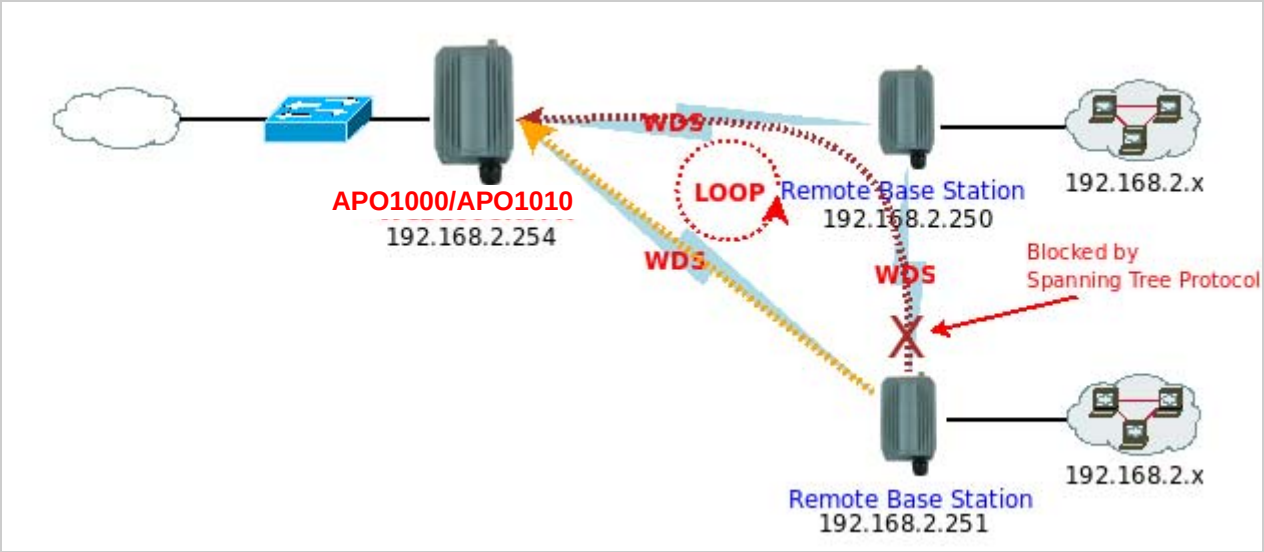
    - ✓ **Hostname :** The Hostname of the LAN port

- **DNS :** Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
  - ➔ **Primary :** The IP address of the primary DNS server.
  - ➔ **Secondary :** The IP address of the secondary DNS server.

- **802.1d Spanning Tree**

  The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.





Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

3.2 Wireless LAN Network Creation

The network manager can configure related wireless settings, **General Settings, Advanced Settings, Virtual AP(VAP) Setting, Security Settings,** and **MAC Filter Settings**.

3.2.1 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

- **MAC address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are 801.11b, 802.11g and 802.11b+802.11g.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from 1 to 54Mbps for the 802.11g and 802.11b/g modes, or 1 to 11Mbps for the 802.11b mode.
- **Country :** Select the desired Country code from the drop-down list; the options are US, ETSI or Japan.
- **Channel :** The channel range will be changed by selecting different country code. The channel range from 1 to 11 for US country code, or 1 to 13 for ETSI country code, or 1 to 14 for JP country code.
- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select the LEVEL 1 to LEVEL 9 that you need for your environment. If you are not sure from which setting to choose, then use the default LEVEL 9 setting.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to all VAPs.

3.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

- **Slot Time :** Slot time is in the range of **1~1489** and set in unit of ***microsecond***. The default value is **20** microsecond.

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **48** microsecond.

  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughputs become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor

performance the ACK Timeout could be made longer to accommodate.

RTS/CTS

Adjustment of RTS Threshold can be done to turn on RTS. CTS Timeout will take effect only when RTS is turned on.

Unlike wired Ethernet, radio transmission may begin with a RTS (Request to Send) frame, and receiver responds with a CTS (Clear to Send) frame. The RTS/CTS mechanism is called *Channel Cleaning*, all stations that received CTS will back off for certain period of time, multiple of the slot time.

Each CTS packet has a NAV (Network Allocation Vector) number n, the channel is reserved for sender and receiver for additional *n-millisecond*. The NAV guarantees the channel is free of interference in next n-millisecond. The last packet of ACK will set NAV to zero, indicated that connection is done and free the channel to others.

- **CTS Timeout :** CTS Timeout is in the range of **1~744** and set in unit of ***microsecond***. The default value is **48** microsecond.

  CTS Timeout will take effect only when RTS is turned on. Adjustment of RTS Threshold can be done to turn on RTS. When hidden wireless stations are present in the wireless network RTS can be considered to turn on to minimize collisions and increase performance. Ensure CTS timeout is long enough to avoid frequent re-transmission of RTS.

Slot Time and ACK/CTS Timeout settings for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **RSSI Threshold :** RSSI Threshold is in the range of **-128~127**.The default value is **24**.

  RSSI is defined as *Received Signal Strength Indication*, when the received signal strength from peer is below this threshold, the peer will be consider as disconnected. Set the threshold higher will make roaming happen earlier, set lower will allow weak signal peer to connect. In normal situation, the longer distance the lower signal strength will be sensed between peers people could consider to lower RSSI threshold to have bigger coverage from the AP or AP client perspective. If it doesn't work well then people could consider to jack up RSSI threshold to have stable smaller coverage and leave AP clients in longer distance to associate with closer AP.

- **Beacon Interval :** Beacon Interval is in the range of **1~5000** and set in unit of ***millisecond***. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1**~**15**. The default is **15**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256**~**2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** RTS Threshold is in the range of **1~2346** byte. The default is **2346** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

  With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **802.11g Protection Mode :** By default, it's "***Enable***". To ***Disable*** is to deactivate 802.11g Protection Mode.

  Protection mode use RTS/CTS to prevent interference with other APs and 802.11b peers, and disabling it will save transmission time used by RTS/CTS. RTS/CTS threshold is effective only when 802.11g protection mode is made enable.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to all VAPs.

3.2.3 Create Virtual AP(VAP)

The APO1000/APO1010 support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into **8** logical access points, each of which can have a different set of security, VLAN tag(ID) and network settings. **Figure 3-2** shows multiple SSIDs with different security type and VLAN settings.

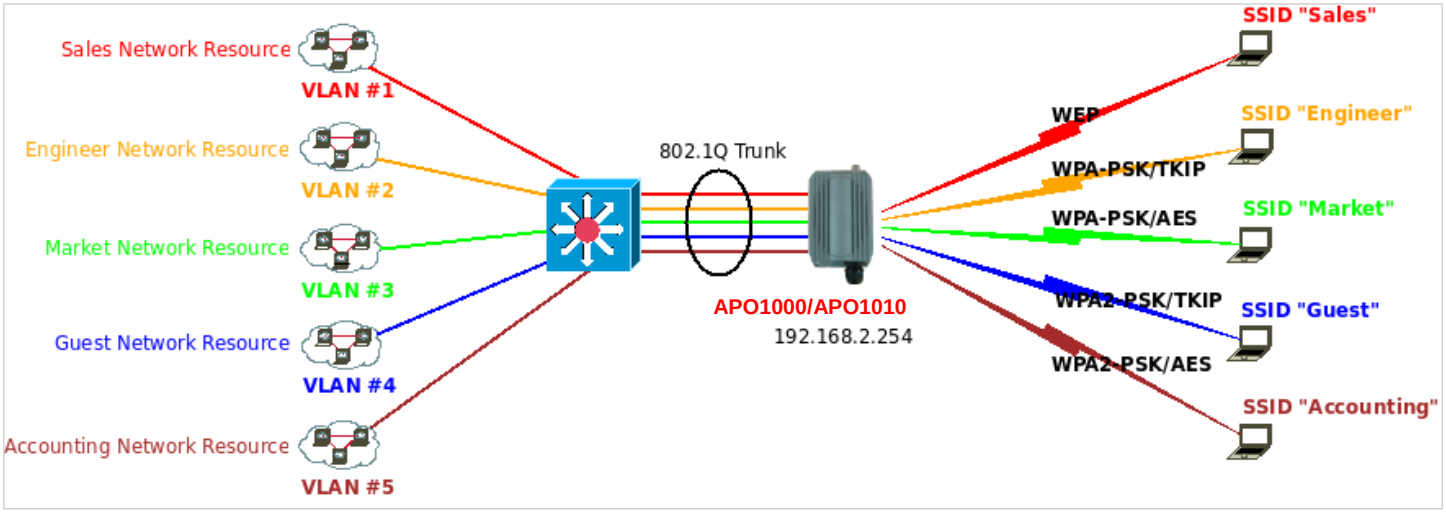


Figure 3-2 Multiple SSIDs with different Security Type and VLAN Tag

3.2.3.1 Virtual AP Overview

The administrator can view all of the Virtual AP's settings via this page.

Please click on **Wireless -> Virtual AP Setup** and the Virtual AP Overview Page appears.

VAP	ESSID	Status	Security Type	MAC Filter	MAC Filter Setup	Edit
VAP0	AP00	On	Disabled	Disable	Setup	Edit
VAP1	AP01	Off	Disabled	Disable	Setup	Edit
VAP2	AP02	Off	Disabled	Disable	Setup	Edit
VAP3	AP03	Off	Disabled	Disable	Setup	Edit
VAP4	AP04	Off	Disabled	Disable	Setup	Edit
VAP5	AP05	Off	Disabled	Disable	Setup	Edit
VAP6	AP06	Off	Disabled	Disable	Setup	Edit
VAP7	AP07	Off	Disabled	Disable	Setup	Edit

- **VAP :** Indicate the system's available Virtual AP
- **ESSID :** Indicate the ESSID of the respective Virtual AP
- **Status :** Indicate the Status of the respective Virtual AP. The **VAP0** always On
- **Security Type :** Indicate an used security type of the respective Virtual AP
- **MAC Filter :** Indicate an used MAC filter of the respective Virtual AP
- **MAC Filter Setup :** Click "**Setup**" button to configure Virtual AP's MAC filter.
- **VAP Edit :** Click "**Edit**" button to configure Virtual AP's settings, including security type.

3.2.3.2 Virtual AP Setup

For each Virtual AP, administrators can configure SSID, VLAN ID(Tag), SSID broadcasting, Maximum number of client associations, security type settings.

Click **Edit** button on the VAP Edit column, and then a Virtual AP setup page appears.

- **ESSID :** Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP clients associated with the specified VAP.
- **Enable VAP :** By default, it's "***Disable***" for **VAP1 ~ VAP7**. The **VAP0** always enabled.

  Select "Enable" to activate VAP or click "Disable" to deactivate this function
- **Hidden SSID :** By default, it's "***Disable***".

  Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.
- **Client Isolation :** By default, it's "***Disable***".

  Select "**Enable"**, all clients will be isolated from each other, which means they can't reach each other.
- **WMM :** By default, it's "***Disable***"***.***

  Select "Enable", then packets with WMM QoS will take higher priority.

  WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. Packets with QoS header including Diffserv/IP ToS and 802.1p will be mapped into 4 Access Categories of WMM, packets without QoS header will be assigned to the Best Effort queue. Please refer to the table below for mapping from 802.1p and ToS mapping to WMM:

Queue	Data Transmitted Clients to AP	IP ToS	802.1P Priority	Priority	Description
AC_BK	Background.	0x08 0x20	1, 2	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort		0, 3	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	0x28 0xa0	4, 5	High	Minimum delay. Time-sensitive video data is automatically sent to this queue

AC_VO	Voice	0x30 0xe0 0x88 0xb8	6, 7	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

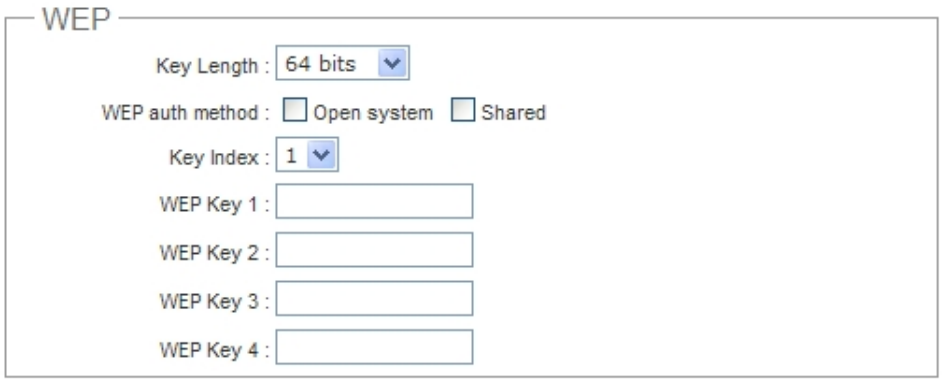
- **IAPP Support :** By default, it's "***Disable***".

  Inter Access-Point Protocol is designed to enforce unique association throughout an ESS(Extended Service Set) and to enforce secure exchange of station's security context between current access point (AP) and new AP during hand off period.

> *IAPP supported only for WPA-PSK/WPA2-PSK, WPA-Enterprise/WPA2-Enterprise and 802.1X security type.*

- **Maximum Clients :** The default value is **32.** You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.
- **VLAN ID(Tag) :** By default, it's selected "***Disable***".

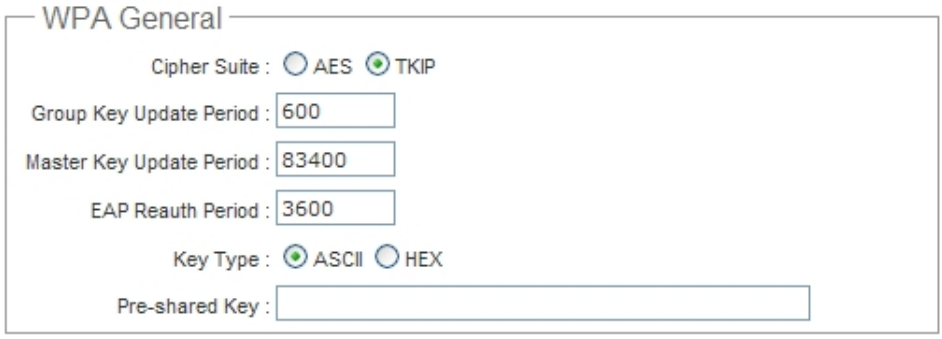
  This system supports tagged Virtual LAN(VLAN). A valid number of **0** to **4094** can be entered after it's enabled. If your network utilize VLANs you could tie a VLAN ID to a specific SSID, and packets from/to wireless clients belonging to that SSID will be tagged with that VLAN ID. This enables security of wireless applications by applying VLAN ID.
- **Security Type :** Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
  - ➔ **Disable :** Data are unencrypted during transmission when this option is selected.
  - ➔ **WEP :** Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key.



  - ✓ **Key Length :** The available options are ***64 bits***, ***128 bits*** or ***152 bits***.
  - ✓ **WEP auth Method :** Enable the desired option among ***Open system*** and ***Shared***.
  - ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
  - ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters
152-bit	32 characters	16 characters

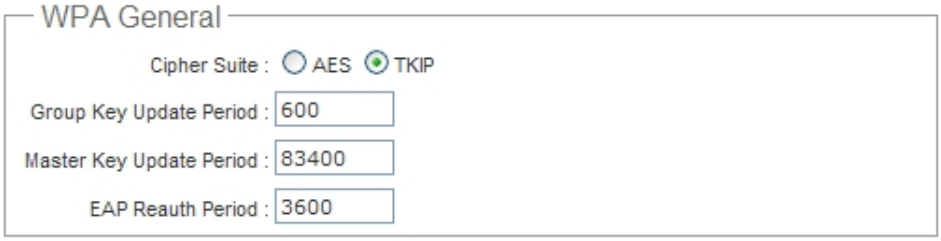
➔ **WPA-PSK/WPA2-PSK :** WPA or WPA2 Algorithms enable the system to access the network by using the WPA-PSK protected access.



- ✓ **Cipher Suite :** By default, it is TKIP. Select either AES or TKIP cipher suites
- ✓ **Group Key Update Period :** By default, it is **600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- ✓ **Master Key Update Period :** By default, it is **83400** seconds. This time interval for rekeying GMK, master key to generate GTKs, in seconds. Enter the time-length required.
- ✓ **Key Type :** Select either **ASCII** or **HEX** format for the Pre-shared Key.
- ✓ **Pre-shared Key :** Enter the pre-shared key; the format shall go with the selected key type.

Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

➔ **WPA-Enterprise/WPA2-Enterprise:** The RADIUS authentication and encryption will apply if either one is selected.

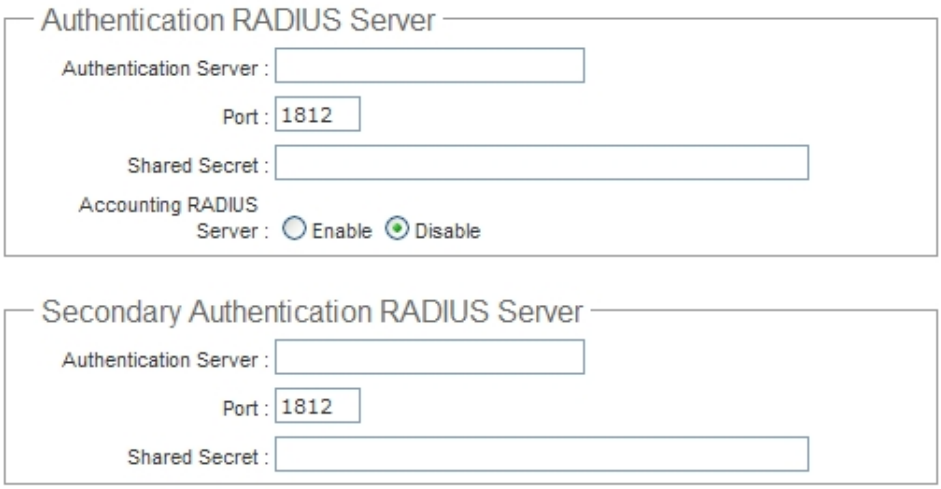


- ✓ **WPA General Settings :**
  - **Cipher Suite :** By default, it is TKIP. Select either AES or TKIP cipher suites
  - **Group Key Update Period :** By default, it's **600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
  - **Master Key Update Period :** By default, it's **83400** seconds. This time interval for rekeying GMK, master

key to generate GTKs, in seconds. Enter the time-length required.

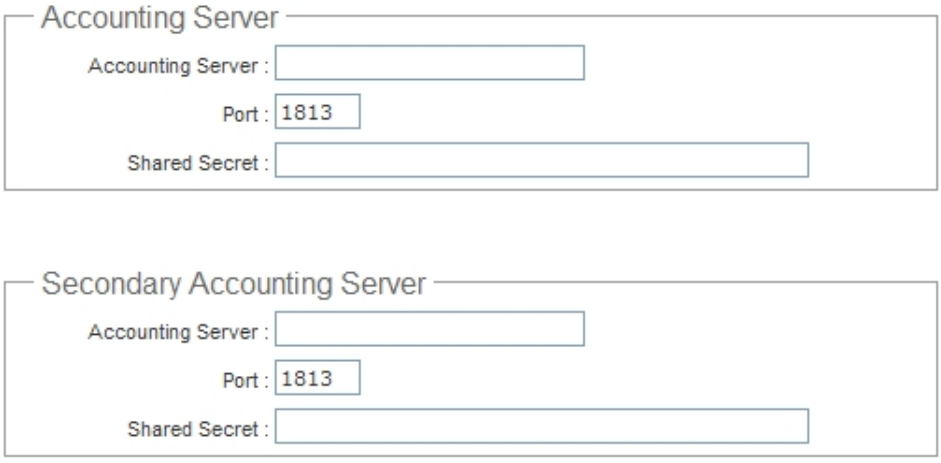
- **EAP Reauth Period :**; By default, it's **3600** seconds; **0** second is to disable EAP Re-authentication.

✓ **Main and secondary Authentication RADIUS Server Settings :**



- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **1** to **64** characters.
- **Accounting Server :** Enable or Disable accounting features in RADIUS server.

✓ **Main or Secondary Accounting RADIUS Server Settings :**



- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port : By default, it's 1813.** The port number used to communicate with RADIUS server.
- **Shared Secret :** A secret key used between system and Accounting RADIUS server. Supports **1** to **64** characters.

➔ **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and

RADIUS settings to complete configuration.

✓ **Dynamic WEP Settings :**

- **W**

  E

  P Key length : The available options are ***64 bits*** or ***128 bits***. The system will automatically generate WEP encryption keys.
- **WEP Key Update Period :** By default, it's 300 seconds; 0 not to rekey.
- **EAP Reauth Period :** By default, it's **3600** seconds; **0** second is to disable EAP Re-authentication.

✓ **Main and Secondary Authentication RADIUS Server Settings :**

- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port : By default, it's 1812.** The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **1** to **64** characters.
- **Accounting Server :** Enable or Disable accounting features in RADIUS server.

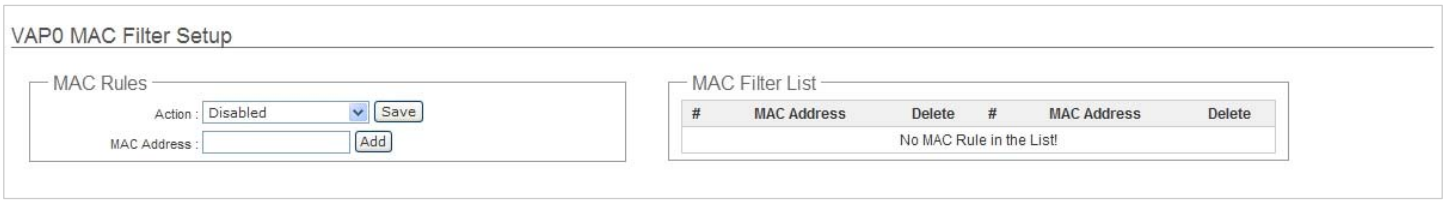
✓ **Main and secondary Accounting RADIUS Server Settings :**

- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port : By default, it's 1813.** The port number used to communicate with RADIUS server.
- **Shared Secret :** A secret key used between system and Accounting RADIUS server. Supports **1** to **64** characters.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

3.2.4 MAC Filter Setup

Continued from the **3.2.3.1 Virtual AP Overview** section, Click **Setup** button on the MAC Filter Setup column, and then a Virtual AP MAC Filter setup page appears. The administrator can allow or reject clients to access each Virtual AP.



- **MAC Filter Setup :** By default, it's "***Disable***". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click ***Save*** button to save your change.

  Two ways to set the MAC filter rules :

  ➔ **Only Allow List MAC**.

  The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

  ➔ **Only Deny List MAC**.

  The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.

- **MAC Address :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons**.**

Click ***Reboot*** button to activate your changes

MAC Access Control is the weakest security approach. WPA or WPA2 security method is highly recommended.

3.3 Wireless Network Expansion

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. ***A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.***

Figure 3-3 shows Point to Multiple Points with different VLAN settings

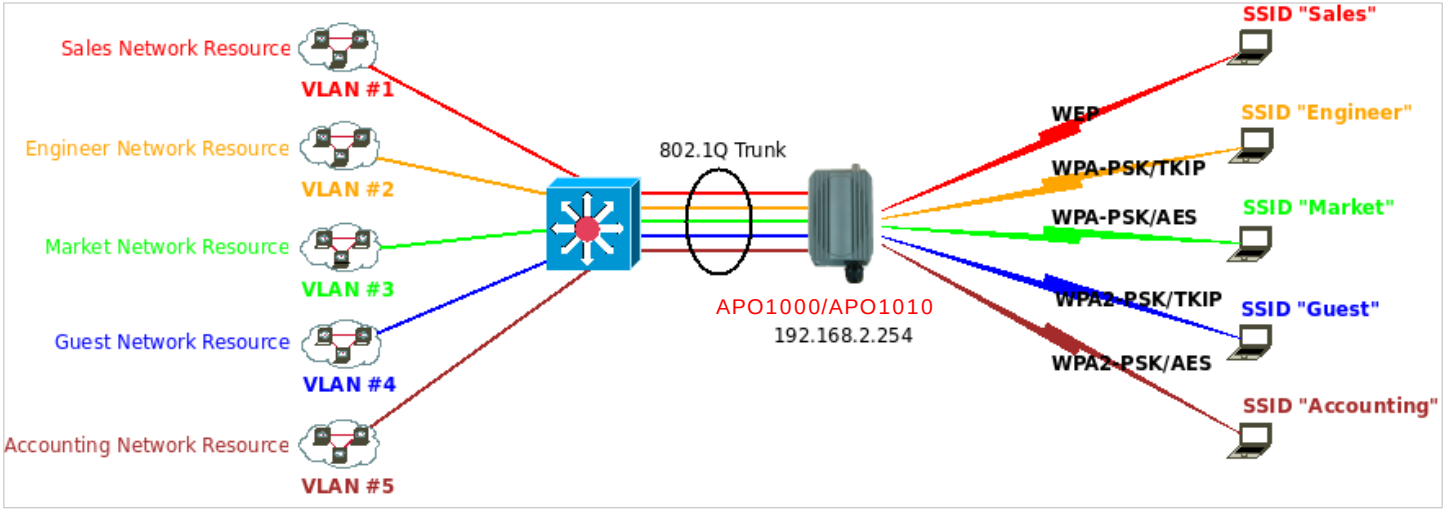
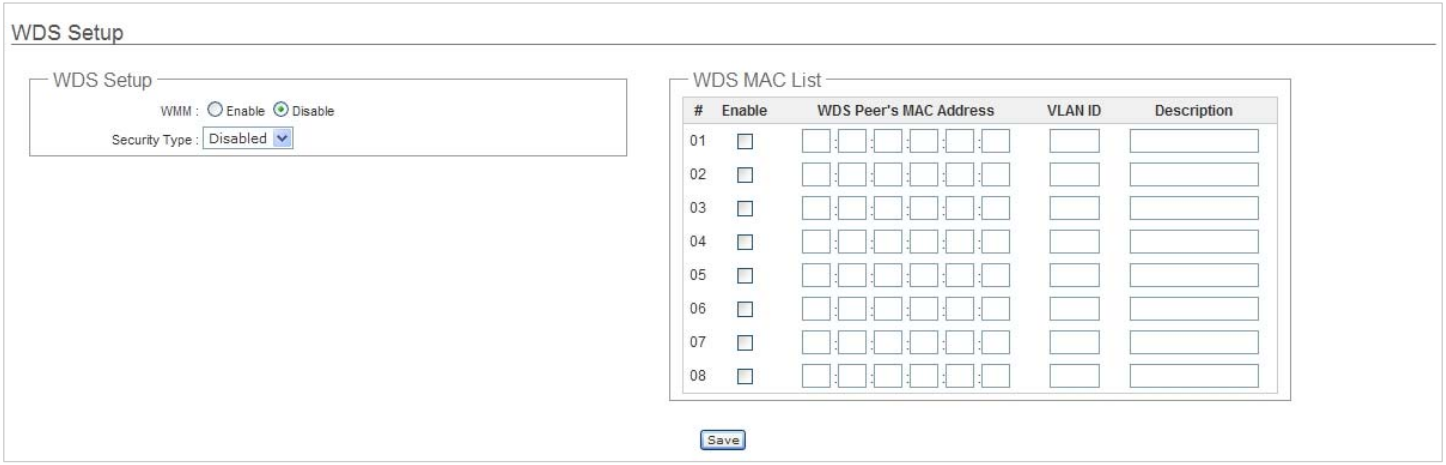


Figure 3-3 Point to Multiple Points with different VLAN Tag

Please click on **Wireless -> WDS Setup** and follow the below setting.



Note that VLAN ID in the WDS MAC List setting will only be tagged to egress packets on the wired Ethernet port. Ensure to match VLAN ID used on the network of the peer. WDS link won't carry tags at all.

- **WMM :** By default, it's "***Disable***".

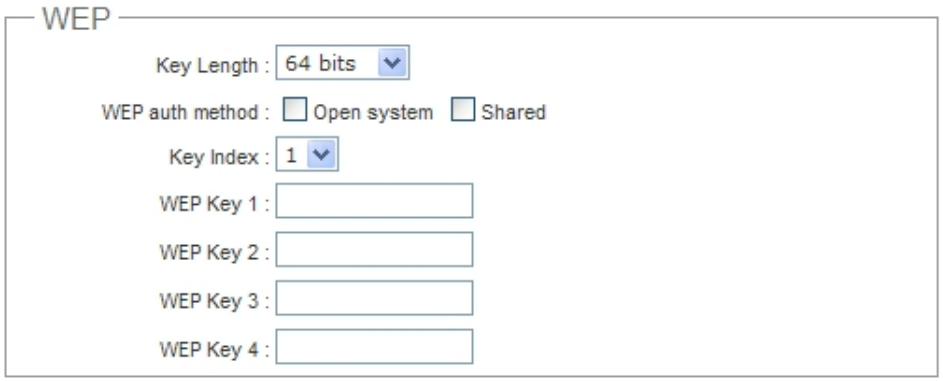
  Select "Enable", then packets with WMM QoS will take higher priority.

WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. Packets with QoS header including Diffserv/IP ToS and 802.1p will be mapped into 4 Access Categories of WMM, packets without QoS header will be assigned to the Best Effort queue. Please refer to the table below for mapping from 802.1p and ToS mapping to WMM:

Queue	Data Transmitted Clients to AP	IP ToS	802.1P Priority	Priority	Description
AC_BK	Background.	0x08 0x20	1, 2	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort		0, 3	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	0x28 0xa0	4, 5	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	0x30 0xe0 0x88 0xb8	6, 7	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

- **Security Type :** Option is "**Disabled**", "**WEP**" or "**AES**" from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.

  ➔ **WEP Key :** Enter **HEX** or **ASCII** WEP key at different length as shown below. This system supports up to 4 sets of WEP keys.



  - ✓ **Key Length :** The available options are ***64 bits***, ***128 bits*** or ***152 bits***.
  - ✓ **WEP auth Method :** Enable the desired option among ***Open system*** and ***Shared***.
  - ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
  - ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters
152-bit	32 characters	16 characters

➔ **AES Key :** Enter **32 HEX** characters AES key.

■ **WDS MAC List**

➔ **Enable :** Click ***Enable*** to create WDS link.

➔ **WDS Peer's MAC Address :** Enter the MAC address of WDS peer.

➔ **VLAN ID :** By default, it's disabled(space) with no VLAN ID. When desired, this system supports tagged VLAN from **0** to **4094**.

➔ **Description :** Description of WDS link.

*The WDS link needs to be set at same **Channel** and with same **Security Type**.*

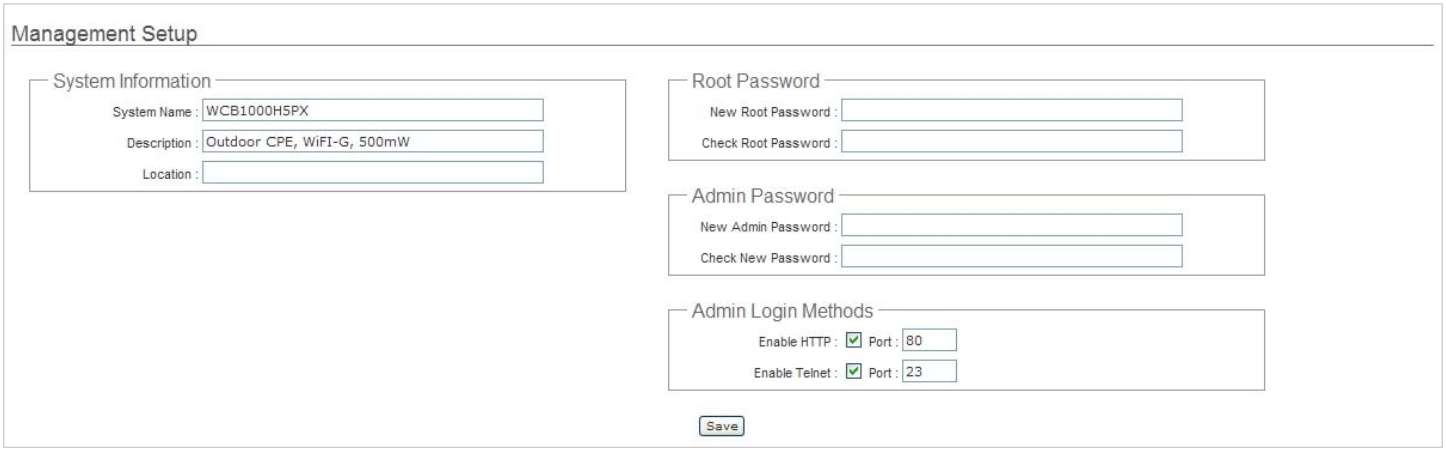
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

3.4 System Management

3.4.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.



- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default one.
  - ➔ **Description :** Provide description of the system.
  - ➔ **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to ***Appendix C. Network manager Privileges***.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only **root** user can enable or disable system login methods and change services port.
  - ➔ **Enable HTTP :** Check to select HTTP Service.
  - ➔ **HTTP Port :** The default is **80** and the range is between 1 ~ 65535.
  - ➔ **Enable Telnet :** Check to select Telnet Service
  - ➔ **Telnet Port :** The default is **23** and the range is between 1 ~ 65535.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

3.4.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

- **Local Time :** Display the current system time.

- **NTP Client :** To synchronize the system time with NTP server.
  - ➔ **Enable :** Check to select NTP client.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time :** Enable or disable Daylight saving.

If the system time from NTS server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

3.4.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

- **UPnP :** By default, it's "***Disable***". Select "**Enable**" or "***Disable"*** of UPnP Service.

  Click ***Save*** button to save changes and click ***Reboot*** button to activate changes

For UPnP to work in Windows XP, the "APO1000" or "APO1010"must be available in "***My Network Places****"*.

If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to ***Appendix D. Using UPnP on Windows XP***

3.4.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP manager and agent. By enabling SNMP function, the administrator can obtain the system information remotely.

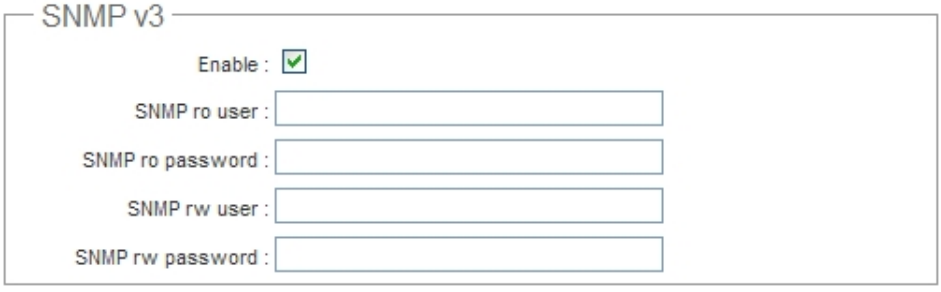
Please click on **System -> SNMP Setup** and follow the below setting.

- **SNMP v2c Enable:** Check to enable SNMP v2c.

  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

  SNMPv3 supports the highest level SNMP security.



  - ➔ **SNMP ro user :** Set a community string to authorize read-only access.
  - ➔ **SNMP ro password :** Set a password to authorize read-only access.
  - ➔ **SNMP rw user :** Set a community string to authorize read/write access.
  - ➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

  - ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
  - ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

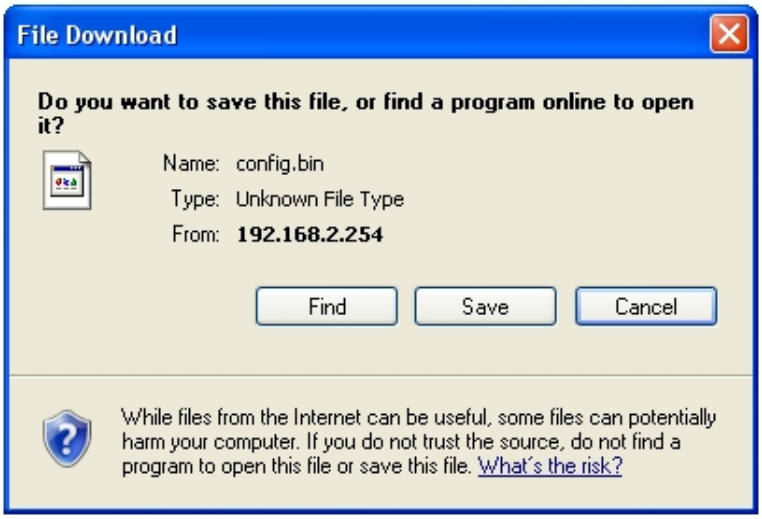
Click ***Save*** button to save changes and click ***Reboot*** button to activate.

3.4.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.

- **Save Settings To PC :** Click ***Save*** button to save the current configuration to a local disk.

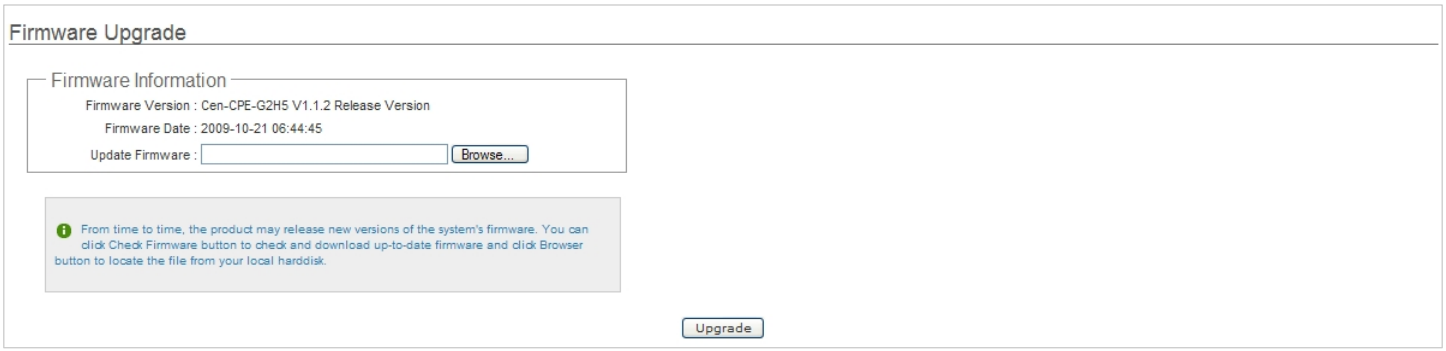


- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

3.4.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **8 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.

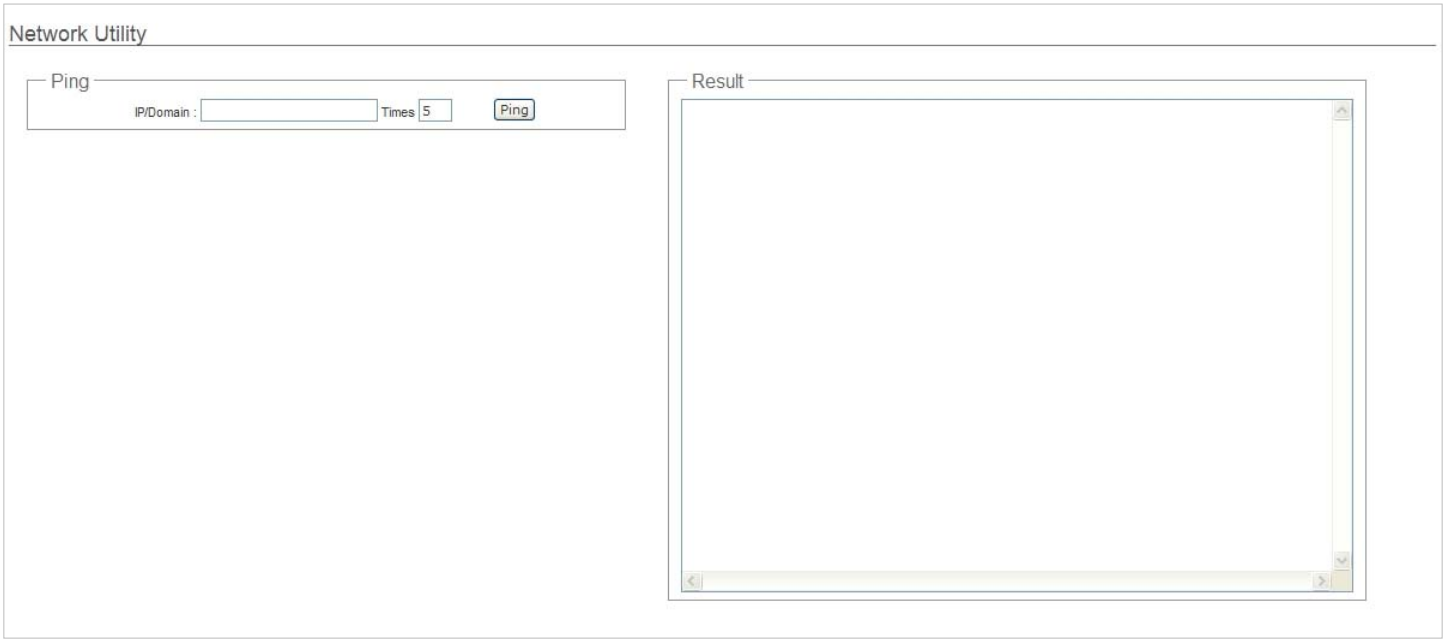


1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*

3.4.7 Network Utility

The administrator can diagnose network connectivity via the PING utility.

Please click on **Utilities -> Network Utility** and follow the below setting.

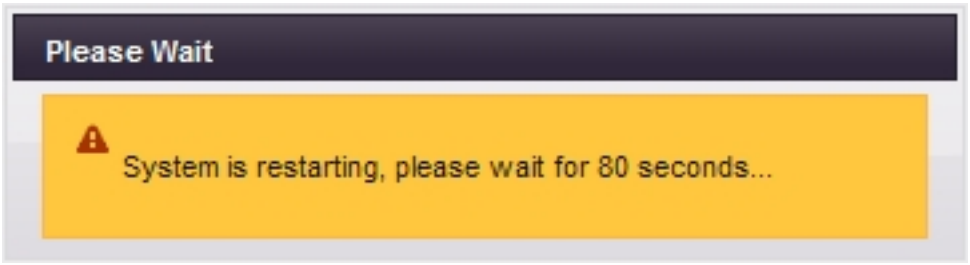


- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count :** By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

3.4.8 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

3.5 System Status

This section breaks down into subsections of ***System Overview***, ***Associated Clients Status***, ***WDS Link Status***, ***Extra Information*** and ***Event Log***.

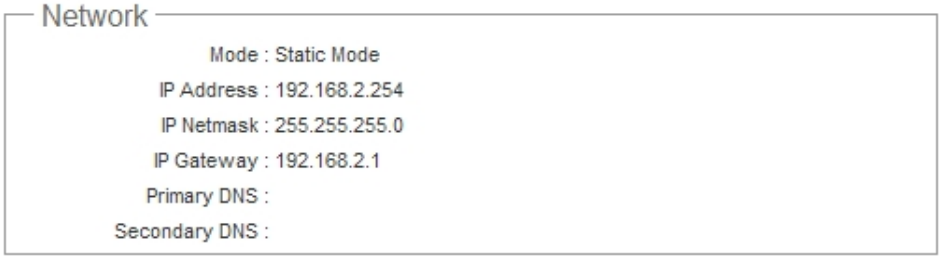
3.5.1 System Overview

Display detailed information of ***System, Network, LAN and Wireless*** in the System Overview page.

- **System :** Display information of the system.

  - ➔ **System Name :** The name of the system.
  - ➔ **Operating Mode :** The mode currently in service.
  - ➔ **Location :** Deployed geographical location.
  - ➔ **Description :** A description of the system.
  - ➔ **Firmware Version :** The current installed firmware version.
  - ➔ **Firmware Date :** The build time of installed firmware.
  - ➔ **Device Time :** The current time of the system.
  - ➔ **System Up Time :** The time period that system has been in service since last reboot.

- **Network Information :** Display information of the Network.



  - ➔ **Mode :** Supports Static or Dynamic modes on the LAN interface.
  - ➔ **IP Address :** The management IP of system. By default, it's 192.168.10.100.
  - ➔ **IP Netmask :** The network mask. By default, it's 255.255.255.0.
  - ➔ **IP Gateway :** The gateway IP address and by default, it's 192.168.10.1.

➔ **Primary DNS :** The primary DNS server in service.

➔ **Secondary DNS :** The secondary DNS server in service.

- **LAN Information :** Display total received and transmitted statistics on the LAN interface.

➔ **MAC Address :** The MAC address of the LAN port.

➔ **Receive bytes :** The total received packets in bytes on the LAN port.

➔ **Receive packets :** The total received packets of the LAN port.

➔ **Transmit bytes :** The total transmitted packets in bytes of the LAN port.

➔ **Transmit packets :** The total transmitted packets of the LAN port.

- **Wireless VAP Information :** Display total received and transmitted statistics on available Virtual AP.

➔ **MAC Address :** The MAC address of the Wireless port. Different MAC address on each Virtual AP

➔ **Receive bytes :**The total received packets in bytes on the Wireless port.

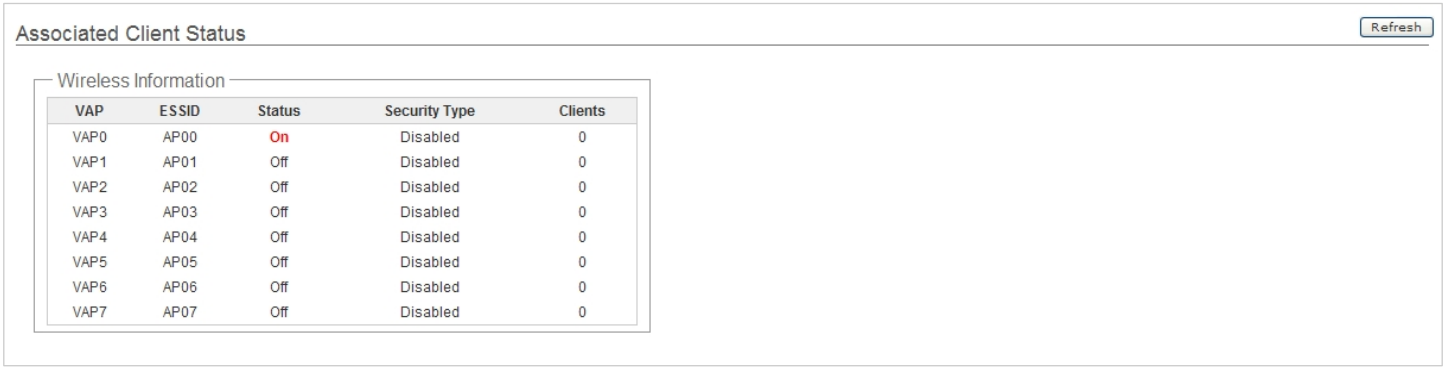
➔ **Receive packets :** The total received packets on the Wireless port.

➔ **Transmit bytes :** The total transmitted packets in bytes on the Wireless port.

➔ **Transmit packets :** The total transmitted packets on the Wireless port.

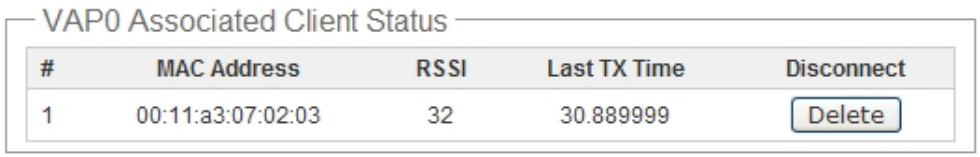
3.5.2 Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with all Virtual AP.



- **VAP Information :** Highlights key VAP information.
  - ➔ **VAP :** Available VAP from VAP0 to VAP7.
  - ➔ **ESSID :** Display name of ESSID for each VAP.
  - ➔ **Status :** On/Off
  - ➔ **Security Type :** Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
  - ➔ **Clients :** Display total number of wireless connections for each VAP.

- **VAP Clients :** Display all associated clients on each Virtual AP.



  - ➔ **MAC Address :** MAC address of associated clients.
  - ➔ **RSSI :** RSSI of from associated clients..
  - ➔ **Last TX Time :** Last inactive time period in seconds for a wireless connection.
  - ➔ **Disconnect :** Click “**Delete**” button to manually disconnect a wireless client in a Virtual AP.

3.5.3 WDS Link Status

On/Off Status, peers MAC Address, Received Signal Strength Indicator (RSSI) and Last TX Time for each WDS are available.

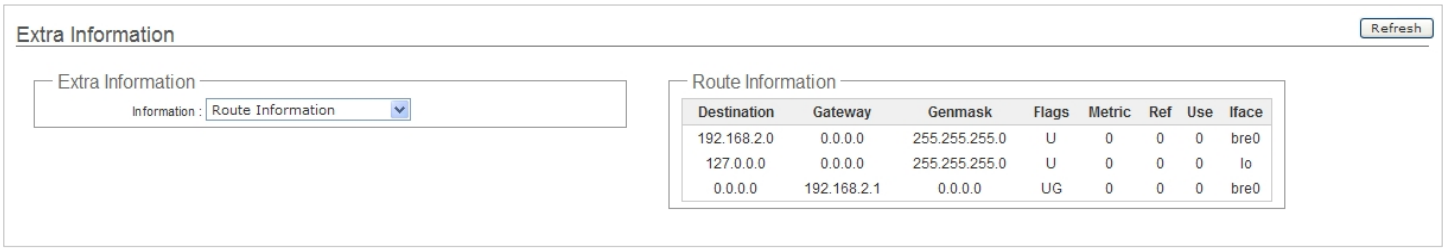
WDS	Status	MAC Address	RSSI	Last TX Time
WDS1	Off	(null)	0	0
WDS2	Off	(null)	0	0
WDS3	Off	(null)	0	0
WDS4	Off	(null)	0	0
WDS5	Off	(null)	0	0
WDS6	Off	(null)	0	0
WDS7	Off	(null)	0	0
WDS8	Off	(null)	0	0

- **WDS :** Maximum supported WDS links.
- **Status :** On/Off.
- **MAC Address :** Display MAC address of WDS peer.
- **RSSI :** Indicate the RSSI of WDS links.
- **Last TX Time :** Last inactive time period in seconds on WDS links.

If display “0” RSSI, you need to check WDS configuration. Things to verify are ***MAC Address***, ***Channel*** *and* ***Security type*****.** Also**,** adjust antenna angle and Tx Power. If display unexpected RSSI, In a long distance application, you might need to adjust ***Slot time, ACK/CTS timeout, and/or RTS threshold.***

3.5.4 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.



- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

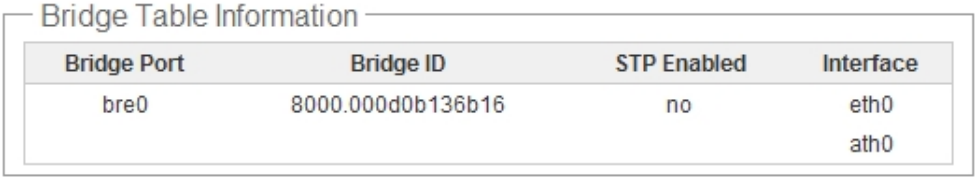
  APO1000/APO1010 could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

  ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

  Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, ath0~ath7 and ath0.wds0~ath0.wds7).



- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

  This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.

Bridge MACs Information

Port No	MAC Address	Local	Ageing Timer
1	00:0d:0b:13:6b:16	yes	0.00
2	00:0d:0b:13:6b:18	yes	0.00
1	00:1a:92:9f:a4:9b	no	0.05

- **Bridge STP Information :** Select "**Bridge STP Information**" on the drop-down list to display a list of bridge STP information.

Bridge STP Information

bre0			
bridge id	8000.000d0b136b16		
designated root	8000.000d0b136b16		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00	gc interval	0.00
hello timer	1.77	tcn timer	0.00
topology change timer	0.00	gc timer	2.77
flags			

eth0 (1)			
port id	8001	state	forwarding
designated root	8000.000d0b136b16	path cost	100
designated bridge	8000.000d0b136b16	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.77
flags			

ath0 (2)			
port id	8002	state	forwarding
designated root	8000.000d0b136b16	path cost	100
designated bridge	8000.000d0b136b16	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.77
flags			

3.5.5 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

- **Time:** The date and time when the event occurred.
- **Facility:** It helps users to identify source of events such “System” or “User”
- **Severity:** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message:** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Chapter 4. WDS Mode Configuration

Please refer to illustrations of the section 1.3 for possible applications in the WDS mode. This section provides detailed explanation for users to configure in the WDS mode with help of illustrations. In the WDS mode, functions listed in the table below are also available from the Web-based GUI interface.

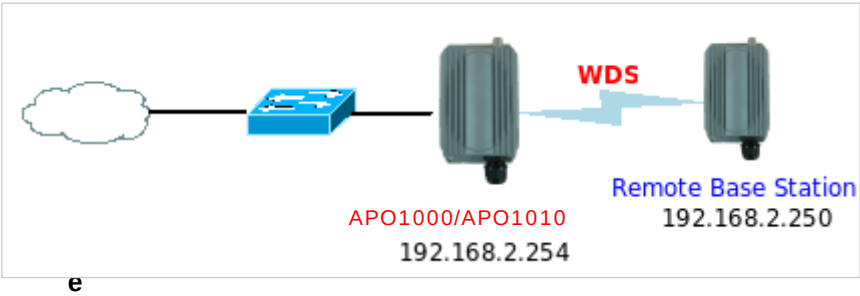
Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Settings	Management	System Overview
	LAN	Advanced Settings	Profiles Settings	WDS Status
	Time Server	WDS Setup	Firmware Upgrade	Extra Info
	SNMP		Network Utility	Event Log
	UPnP		Reboot	

Table 4-1: WDS Mode Functions

4.1 External Network Connection

4.1.1 Network Requirement

You could expand your Ethernet network via WDS link. In this mode, the APO1000/APO1010 connects directly to a wired LAN, and wirelessly bridges to a remote access point via a WDS link as shown in Figure 4-1. In the mode, it can't associate with any wireless clients.



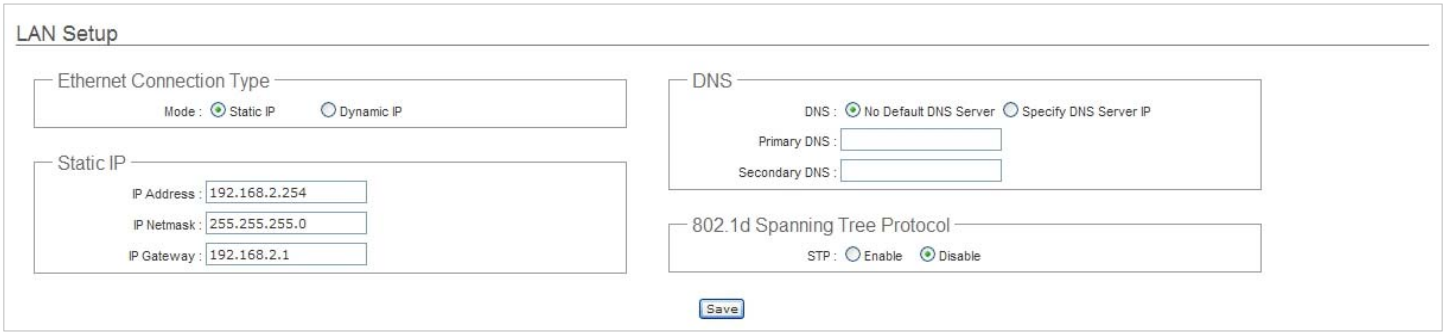
e

4-1 Point to Point Configuration

4.1.2 Configure LAN IP

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.



➔ **Mode :** Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .

➔ **Static IP :** The administrator can manually setup the LAN IP address when static IP is available/ preferred.

- ✓ **IP Address :** The IP address of the LAN port; default IP address is 192.168.10.100
- ✓ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
- ✓ **IP Gateway :** The default gateway of the LAN port; default Gateway is 192.168.10.1

➔ **Dynamic IP :** This configuration type is applicable when the APO1000/APO1010 is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

➔ **Hostname :** The Hostname of the LAN port

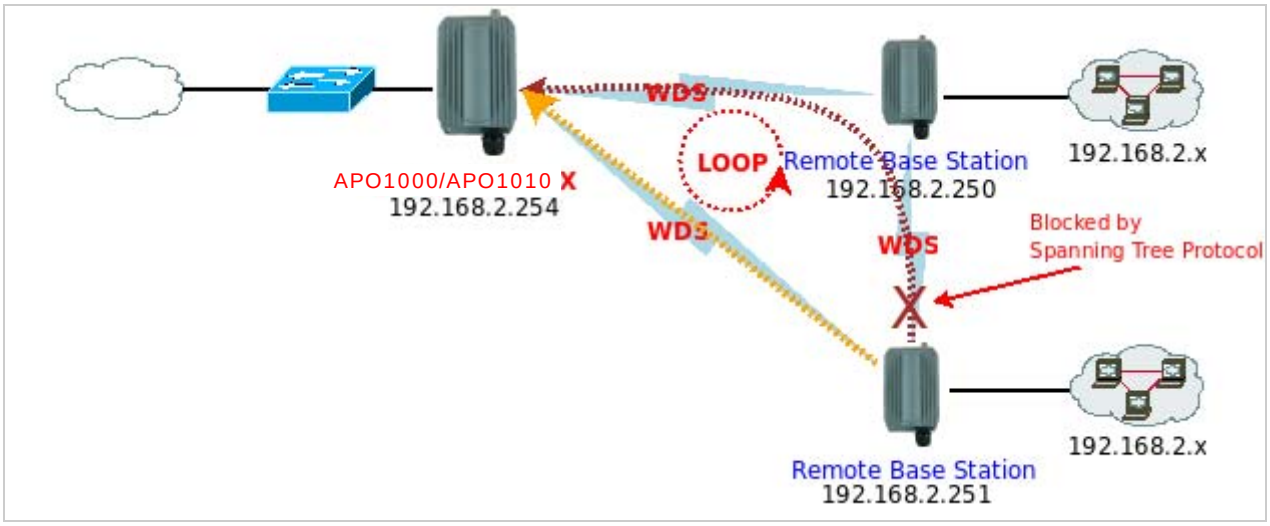
■ **DNS :** Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.

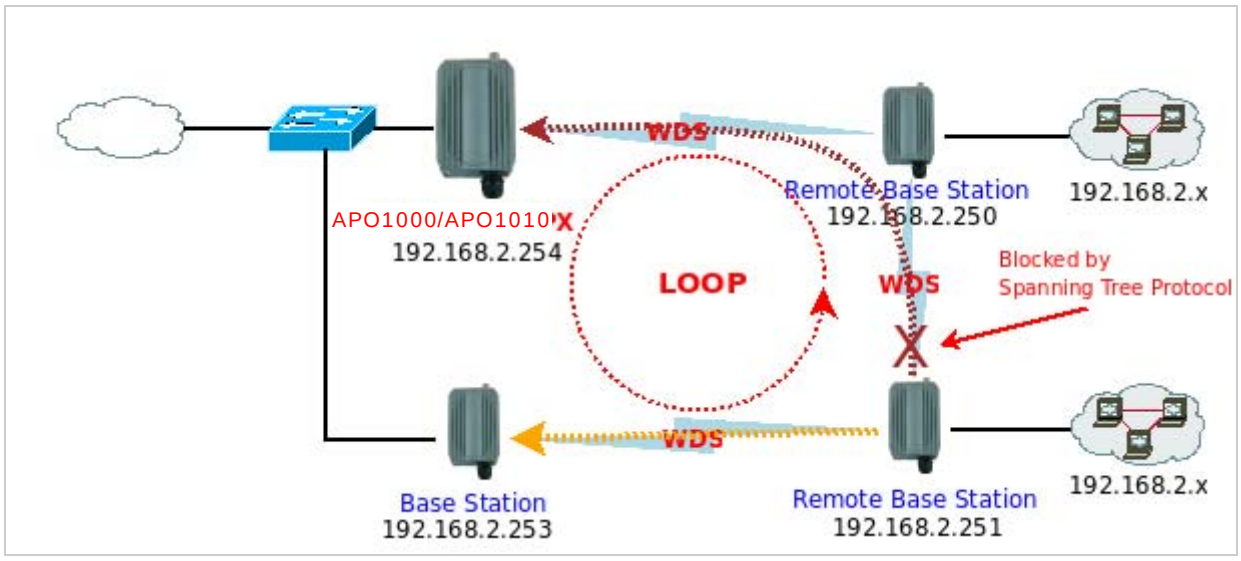
➔ **Primary :** The IP address of the primary DNS server.

➔ **Secondary :** The IP address of the secondary DNS server.

➔ **802.1d Spanning Tree**

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.





Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.2 Wireless Network Expansion

The network manager can configure related wireless settings, **General Settings, Advanced Settings, Virtual AP Setting** and **Security Settings**.

4.2.1 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

- **MAC address :** The MAC address of the Wireless interface is displayed here.
- **Band Mode :** Select an appropriate wireless band; bands available are 801.11b, 802.11g and 802.11b+802.11g.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from 1 to 54Mbps for 802.11g and 802.11b/g modes, or 1 to 11Mbps for 802.11b mode.
- **Country :** Select the desired Country code from the drop-down list; the options are US, ETSI or Japan.
- **Channel :** The channel range will be changed by selecting different country code. The channel range from 1 to 11 for US country code, or 1 to 13 for ETSI country code, or 1 to 14 for JP country code.

The Channel 14 for Japan only used on IEEE802.11b only

- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select the LEVEL 1 to LEVEL 9 you needed for your environment. If you are not sure of which setting to choose, then keep the default setting, LEVEL 9.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to all WDS links.

4.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

- **Slot Time :** Slot time is in the range of **1~1489** and set in unit of ***microsecond***. The default value is **20** microsecond.

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **48** microsecond.

  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughputs become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor

performance the ACK Timeout could be made longer to accommodate.

RTS/CTS

Adjustment of RTS Threshold can be done to turn on RTS. CTS Timeout will take effect only when RTS is turned on.

Unlike wired Ethernet, radio transmission may begin with a RTS (Request to Send) frame, and receiver responds with a CTS (Clear to Send) frame. The RTS/CTS mechanism is called *Channel Cleaning*, all stations that received CTS will back off for certain period of time, multiple of the slot time.

Each CTS packet has a NAV (Network Allocation Vector) number n, the channel is reserved for sender and receiver for additional *n-millisecond*. The NAV guarantees the channel is free of interference in next n-millisecond. The last packet of ACK will set NAV to zero, indicated that connection is done and free the channel to others.

- **CTS Timeout :** CTS Timeout is in the range of **1~744** and set in unit of ***microsecond***. The default value is **48** microsecond.

  CTS Timeout will take effect only when RTS is turned on. Adjustment of RTS Threshold can be done to turn on RTS. When hidden wireless stations are present in the wireless network RTS can be considered to turn on to minimize collisions and increase performance. Ensure CTS timeout is long enough to avoid frequent re-transmission of RTS.

Slot Time and ACK/CTS Timeout settings for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **RSSI Threshold :** RSSI Threshold is in the range of **-128~127**.The default value is **24**.

  RSSI is defined as *Received Signal Strength Indication*, when the received signal strength from peer is below this threshold, the peer will be consider as disconnected. Set the threshold higher will make roaming happen earlier, set lower will allow weak signal peer to connect. In normal situation, the longer distance the lower signal strength will be sensed between peers people could consider to lower RSSI threshold to have bigger coverage from the AP or AP client perspective. If it doesn't work well then people could consider to jack up RSSI threshold to have stable smaller coverage and leave AP clients in longer distance to associate with closer AP.

- **Beacon Interval :** Beacon Interval is in the range of **1~5000** and set in unit of ***millisecond***. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1**~**15**. The default is **15**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

  A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256**~**2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** RTS Threshold is in the range of **1~2346** byte. The default is **2346** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

  With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **802.11g Protection Mode :** By default, it's "***Enable***". To ***Disable*** is to deactivate 802.11g Protection Mode.

  Protection mode use RTS/CTS to prevent interference with other APs and 802.11b peers, and disabling it will save transmission time used by RTS/CTS. RTS/CTS threshold is effective only when 802.11g protection mode is made enable.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to all WDS links.

4.2.3 WDS Setup

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. ***A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.***

Figure 4-2 shows Point to Multiple Points with different VLAN settings

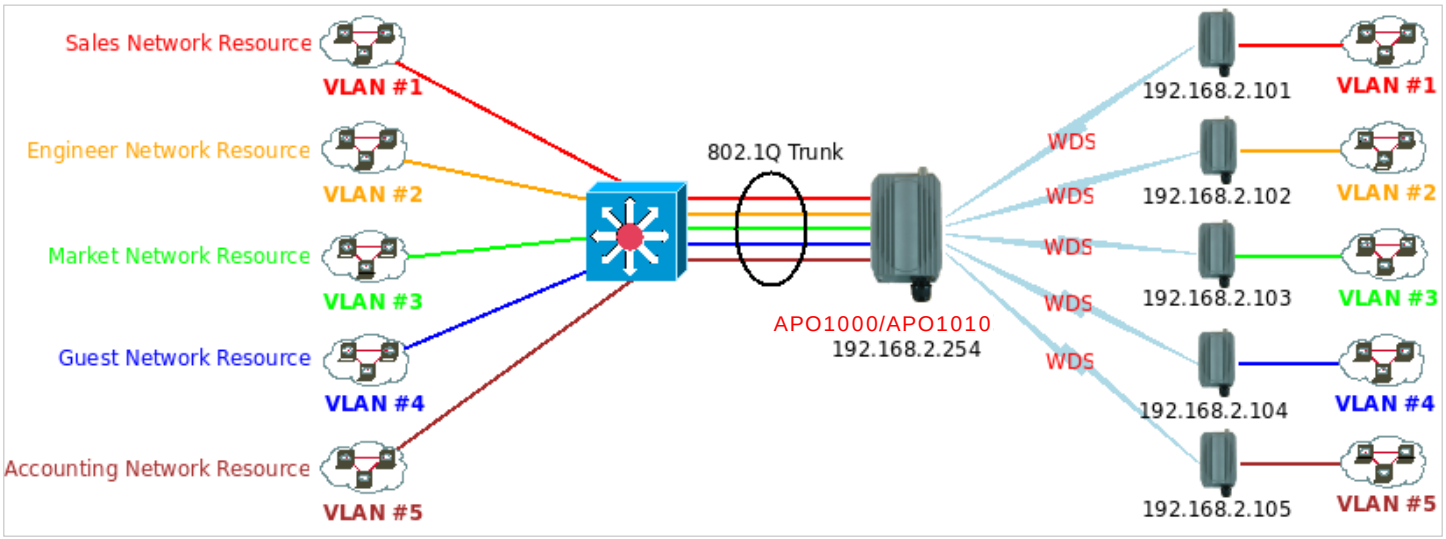
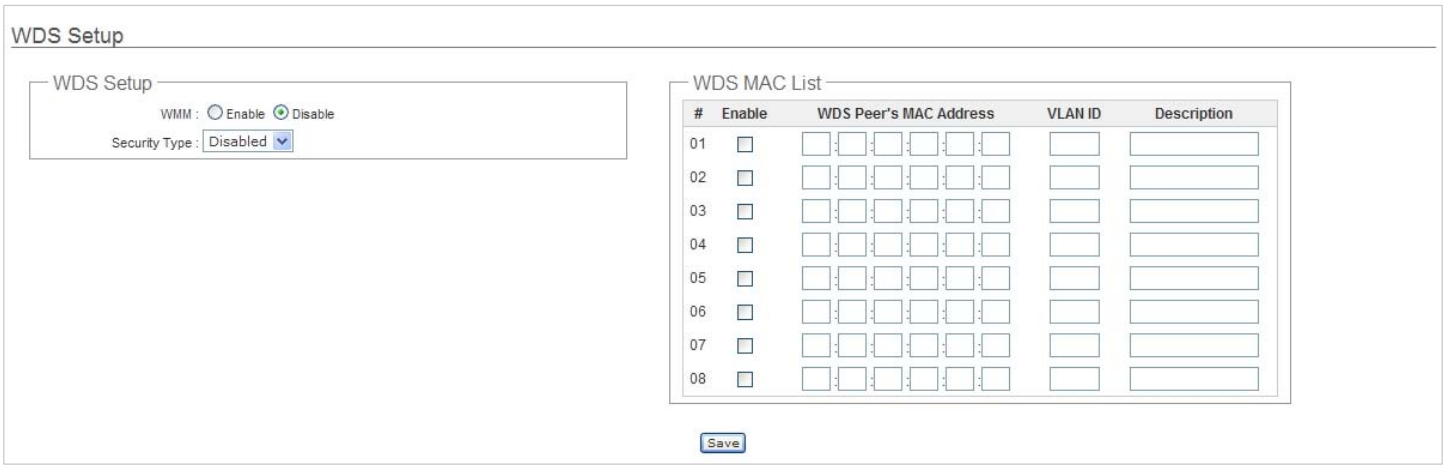


Figure 4-2 Point to Multiple Points with different VLAN Tag

Please click on **Wireless -> WDS Setup** and follow the below setting.



Note that VLAN ID in the WDS MAC List setting will only be tagged to egress packets on the wired Ethernet port. Ensure to match VLAN ID used on the network of the peer. WDS link won't carry tags at all.

- **WMM :** By default, it's "***Disable***".

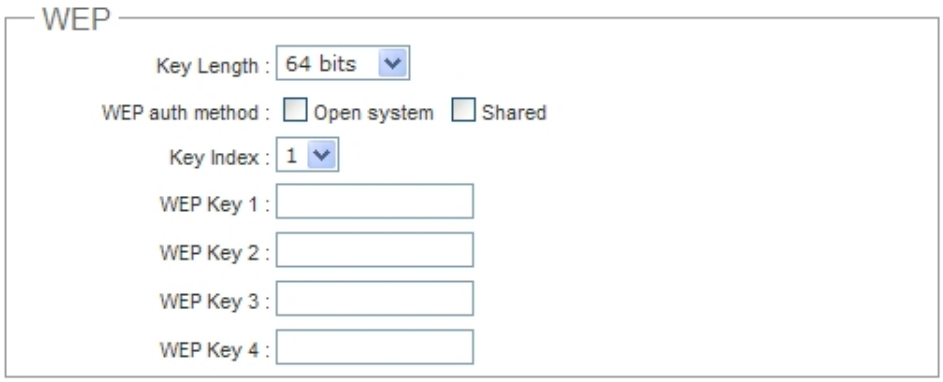
  Select "Enable", then packets with WMM QoS will take higher priority.

WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. Packets with QoS header including Diffserv/IP ToS and 802.1p will be mapped into 4 Access Categories of WMM, packets without QoS header will be assigned to the Best Effort queue. Please refer to the table below for mapping from 802.1p and ToS mapping to WMM:

Queue	Data Transmitted Clients to AP	IP ToS	802.1P Priority	Priority	Description
AC_BK	Background.	0x08 0x20	1, 2	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort		0, 3	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	0x28 0xa0	4, 5	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	0x30 0xe0 0x88 0xb8	6, 7	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

- **Security Type :** Option is "**Disabled**", "**WEP**" or "**AES**" from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.

  ➔ **WEP Key :** Enter **HEX** or **ASCII** WEP key at different length as shown below. This system supports up to 4 sets of WEP keys.



  ✓ **Key Length :** The available options are ***64 bits***, ***128 bits*** or ***152 bits***.

  ✓ **WEP auth Method :** Enable the desired option among ***Open system*** and ***Shared***.

  ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.

  ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters
152-bit	32 characters	16 characters

  ➔ **AES Key :** Enter **32 HEX** characters AES key.

- **WDS MAC List**
  - ➔ **Enable :** Click ***Enable*** to create WDS link.
  - ➔ **WDS Peer's MAC Address :** Enter the MAC address of WDS peer.
  - ➔ **VLAN ID :** By default, it's disabled(space) with no VLAN ID. When desired, this system supports tagged VLAN from **0** to **4094**.
  - ➔ **Description :** Description of WDS link.

*The WDS link needs to be set at same **Channel** and **Security Type**.*

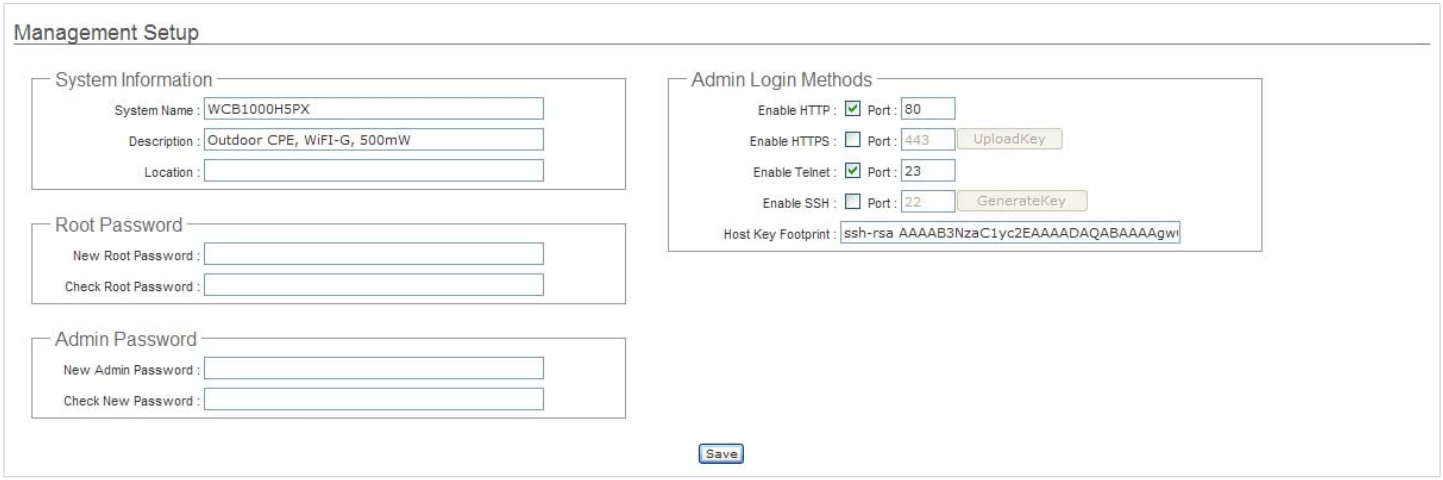
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.3 System Management

4.3.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.



- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default one.
  - ➔ **Description :** Provide description of the system.
  - ➔ **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to ***Appendix C. Network manager Privileges***.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only **root** user can enable or disable system login methods and change services port.
  - ➔ **Enable HTTP :** Check to select HTTP Service.
  - ➔ **HTTP Port :** The default is **80** and the range is between 1 ~ 65535.
  - ➔ **Enable HTTPS :** Check to select HTTPS Service
  - ➔ **HTTPS Port :** The default is **443** and the range is between 1 ~ 65535.

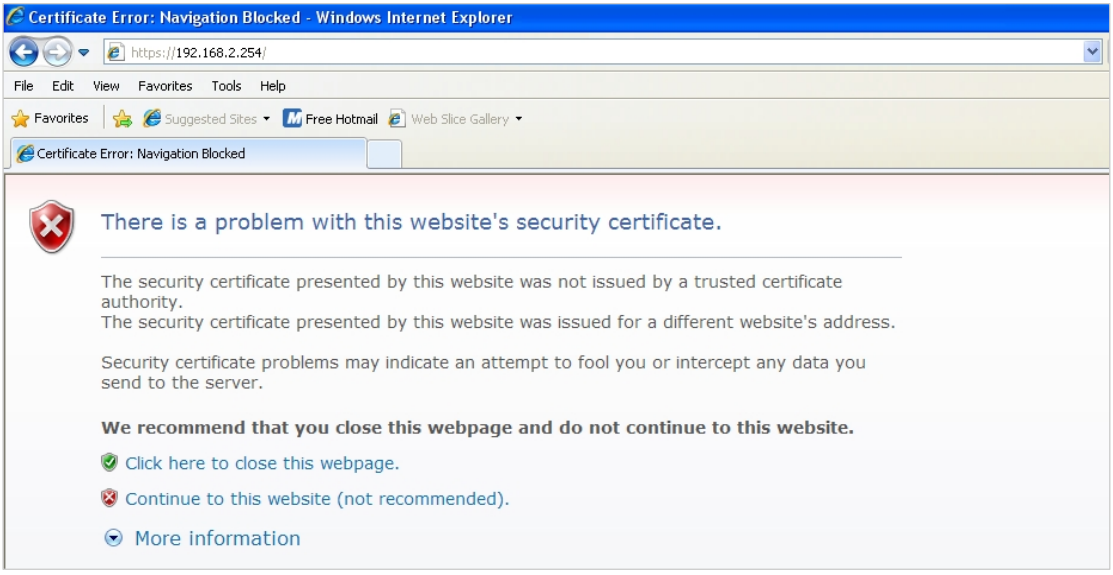
*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

  - ➔ **Enable Telnet :** Check to select Telnet Service
  - ➔ **Telnet Port :** The default is **23** and the range is between 1 ~ 65535.
  - ➔ **Enable SSH :** Check to select SSH Service
  - ➔ **SSH Port :** Please The default is **22** and the range is between 1 ~ 65535.

*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's Web GUI (https://192.168.2.254). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click "***Continue to this website***" to access the system's Web GUI. The system's Overview page will appear.

4.3.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

- **Local Time :** Display the current system time.

- **NTP Client :** To synchronize the system time with NTP server.
  - ➔ **Enable :** Check to select NTP client.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time :** Enable or disable Daylight saving.

If the system time from NTS server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

4.3.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

- **UPnP :** By default, it's "***Disable***". Select "**Enable**" or "***Disable"*** of UPnP Service.

  Click ***Save*** button to save changes and click ***Reboot*** button to activate changes

For UPnP to work in Windows XP, the "APO1000" or "APO1010" must be available in "***My Network Places***".

If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to ***Appendix D. Using UPnP on Windows XP***

4.3.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

- **SNMP v2c Enable :** Check to enable SNMP v2c.

  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

  SNMPv3 supports the highest level SNMP security.

  - ➔ **SNMP ro user :** Set a community string to authorize read-only access.
  - ➔ **SNMP ro password :** Set a password to authorize read-only access.
  - ➔ **SNMP rw user :** Set a community string to authorize read/write access.
  - ➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

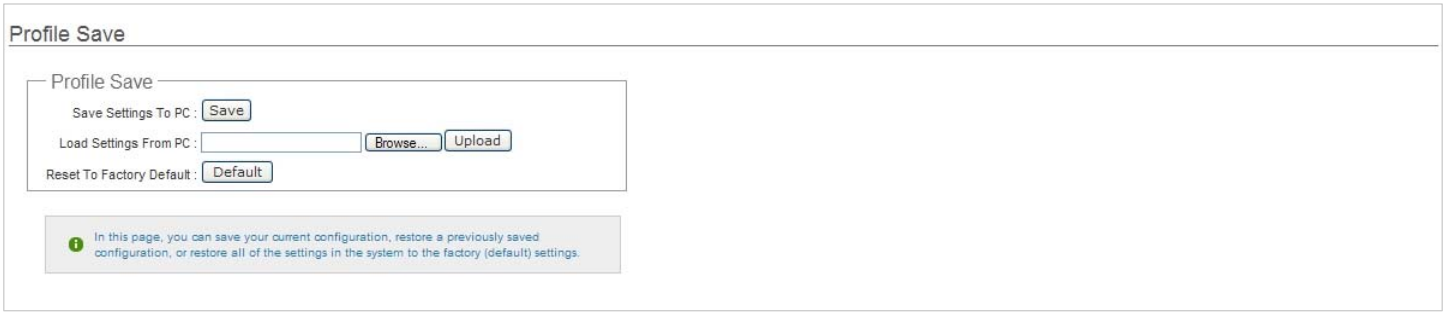
- ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

Click ***Save*** button to save changes and click ***Reboot*** button to activate.

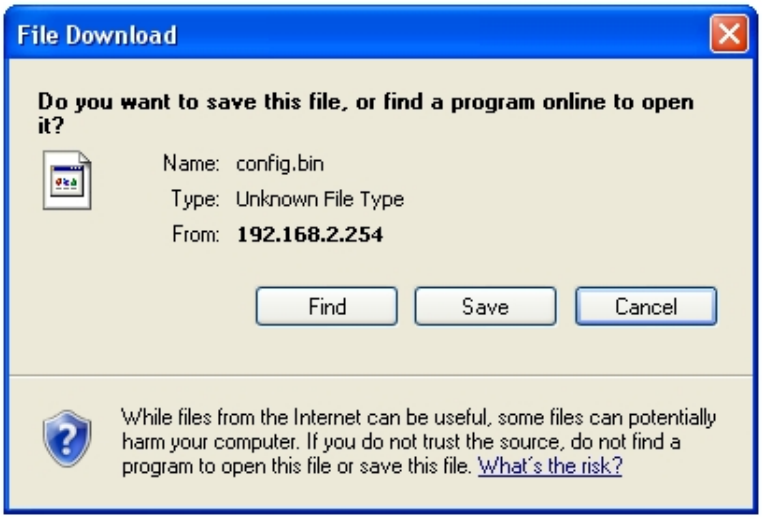
4.3.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.



- **Save Settings to PC :** Click ***Save*** button to save the current configuration to a local disk.

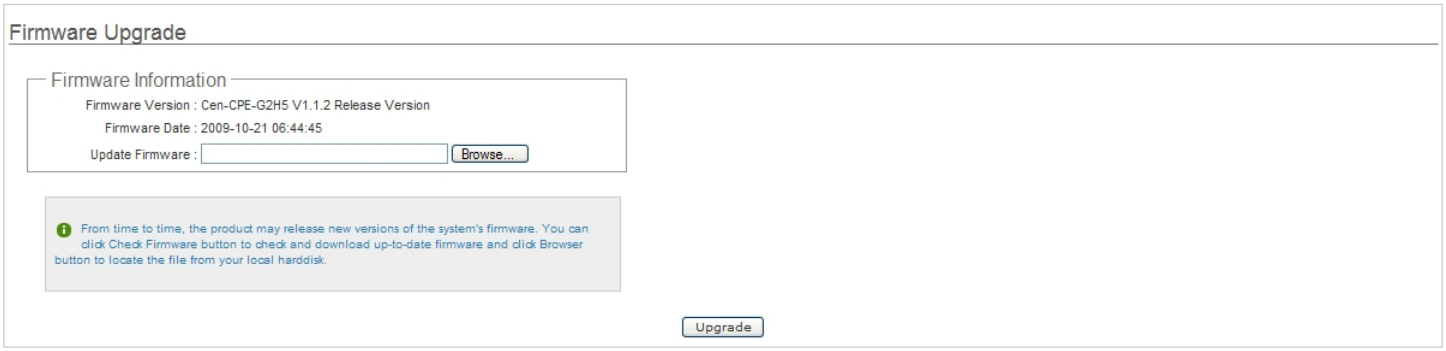


- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

4.3.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **8 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.

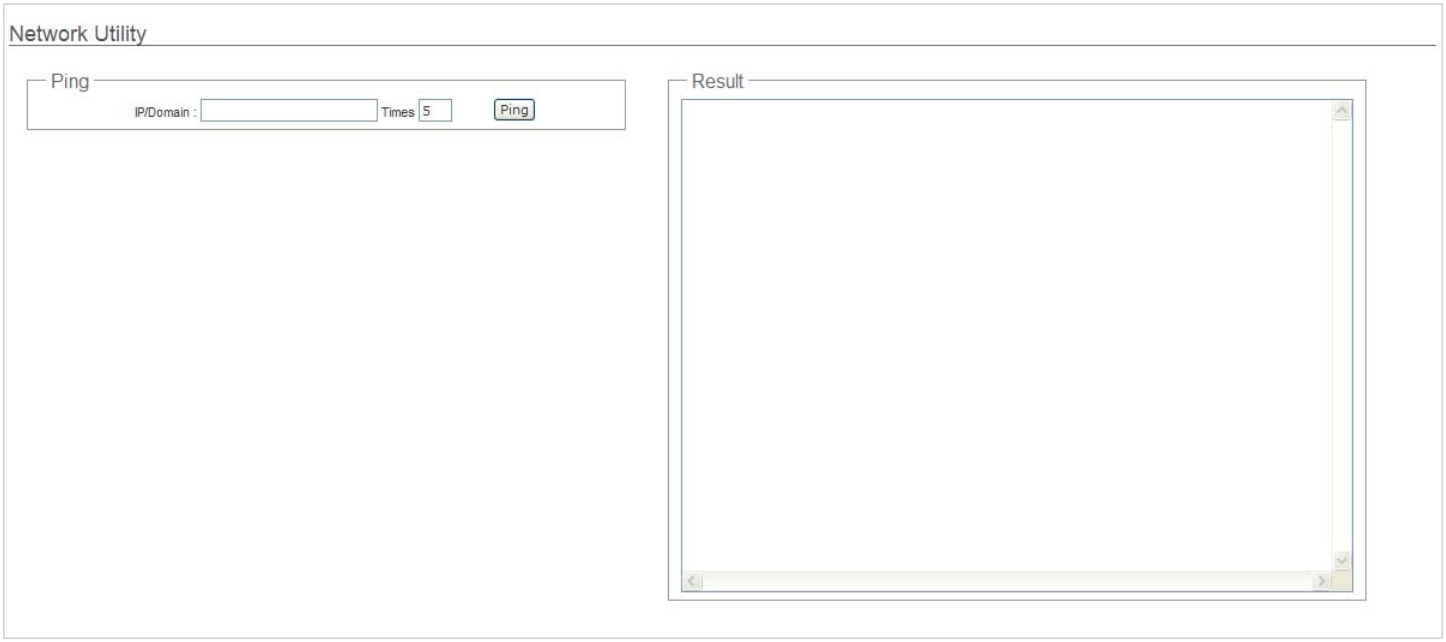


1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding.*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*

4.3.7 Network Utility

The administrator can diagnose network connectivity via the PING utility.

Please click on **Utilities -> Network Utility** and follow the below setting.

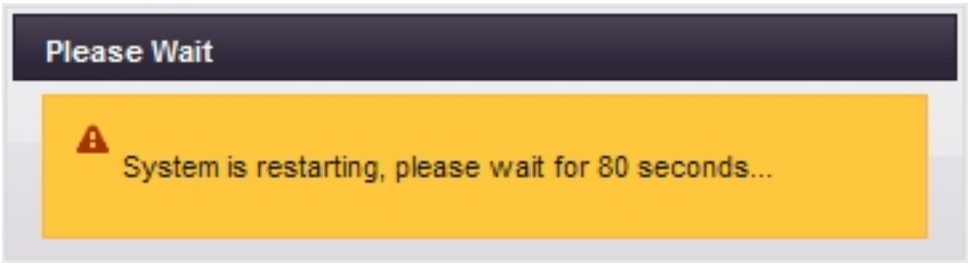


- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count :** By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

4.3.8 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

4.4 System Status

This section breaks down into subsections of ***System Overview***, ***WDS Link Status***, ***Extra Information*** and ***Event Log***.

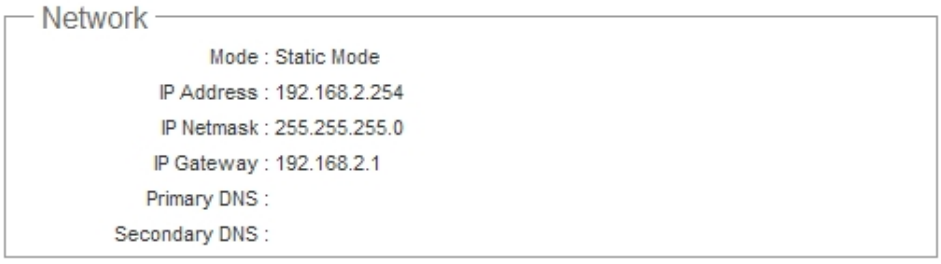
4.4.1 System Overview

Detailed information on **System**, **Network**, **LAN Information** and **Wireless Information** can be reviewed via this page.

- **System :** Display the information of the system.

  - ➔ **System Name :** The name of the system.
  - ➔ **Operating Mode :** The mode currently in service.
  - ➔ **Location :** The reminding note on the geographical location of the system.
  - ➔ **Description :** The reminding note of the system.
  - ➔ **Firmware Version :** The current firmware version installed.
  - ➔ **Firmware Date :** The build time of the firmware installed.
  - ➔ **Device Time :** The current time of the system.
  - ➔ **System Up Time :** The time period that system has been in service since last reboot.

- **Network Information :** Display the information of the Network.



  - ➔ **Mode :** Supports Static or Dynamic modes on the LAN interface.
  - ➔ **IP Address :** The management IP of system. By default, it's 192.168.10.100.
  - ➔ **IP Netmask :** The network mask. By default, it's 255.255.255.0.
  - ➔ **IP Gateway :** The gateway IP address and by default, it's 192.168.10.1.
  - ➔ **Primary DNS :** The primary DNS server in service.
  - ➔ **Secondary DNS :** The secondary DNS server in service.

- **LAN Information :** Display total received and transmitted statistics on the LAN interface.

  - ➔ **MAC Address :** The MAC address of the LAN port.
  - ➔ **Receive bytes :** The total received packets in bytes on the LAN port.
  - ➔ **Receive packets :** The total received packets of the LAN port.
  - ➔ **Transmit bytes :** The total transmitted packets in bytes of the LAN port.
  - ➔ **Transmit packets :** The total transmitted packets of the LAN port.

4.4.2 WDS Link Status

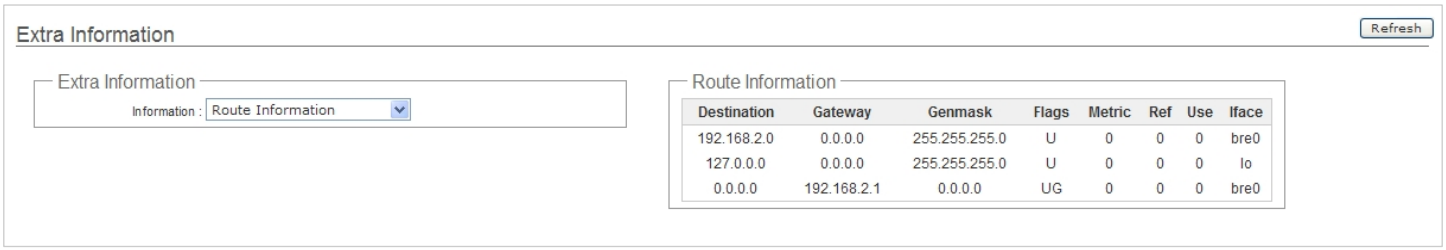
On/Off Status, peers MAC Address, Received Signal Strength Indicator(RSSI) and Last TX Time for each WDS are available.

- **WDS :** Maximum supported WDS links.
- **Status :** On/Off.
- **MAC Address :** Display MAC address of WDS peer.
- **RSSI :** Indicate the RSSI of WDS links.
- **Last TX Time :** Last inactive time period in seconds on WDS links.

If display “0” RSSI, you need to check WDS configuration. Things to verify are ***MAC Address***, ***Channel*** *and* ***Security type*****.** Also**,** adjust antenna angle and Tx Power. If display unexpected RSSI, In a long distance application, you might need to adjust ***Slot time, ACK/CTS timeout, and/or RTS threshold.***

4.4.3 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.



- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

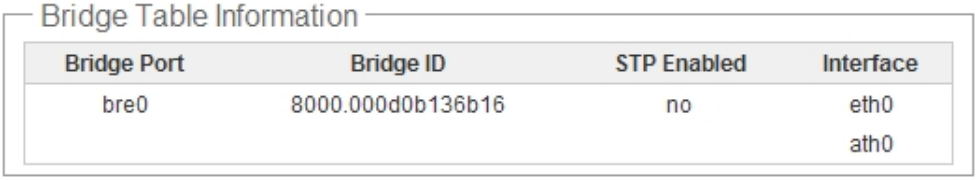
  APO1000/APO1010 could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

  ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

  Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, ath0.wds0~ath0.wds7).



- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

  This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.

Bridge MACs Information

Port No	MAC Address	Local	Ageing Timer
1	00:0d:0b:13:6b:16	yes	0.00
2	00:0d:0b:13:6b:18	yes	0.00
1	00:1a:92:9f:a4:9b	no	0.05

- **Bridge STP Information :** Select "**Bridge STP Information**" on the drop-down list to display a list of bridge STP information.

Bridge STP Information

bre0			
bridge id	8000.000d0b136b16		
designated root	8000.000d0b136b16		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00	gc interval	0.00
hello timer	1.77	tcn timer	0.00
topology change timer	0.00	gc timer	2.77
flags			

eth0 (1)			
port id	8001	state	forwarding
designated root	8000.000d0b136b16	path cost	100
designated bridge	8000.000d0b136b16	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.77
flags			

ath0 (2)			
port id	8002	state	forwarding
designated root	8000.000d0b136b16	path cost	100
designated bridge	8000.000d0b136b16	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.77
flags			

4.4.4 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as troubleshooting tool when issues are experienced in system.

- **Time:** The date and time when the event occurred.
- **Facility:** It helps users to identify source of events such “System” or “User”
- **Severity:** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message:** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Chapter 5. CPE Mode Configuration

When CPE mode is chosen, the system can be configured as a Customer Premises Equipment(CPE). This section provides detailed explanation for users to configure in the CPE mode with help of illustrations. In the CPE mode, functions listed in the table below are also available from the Web-based GUI interface.

OPTION	System	Wireless	Advance	Utilities	Status
Functions	Operating Mode	General Setup	DMZ	Profiles Settings	System Overview
	WAN	Advanced Setup	IP Filter Setup	Firmware Upgrade	DHCP Clients
	LAN	Site Survey	MAC Filter Setup	Network Utility	Extra Info
	DDNS		Virtual Server	Reboot	Event Log
	Management				
	Time Server				
	SNMP				
	UPNP				

Table 5-1: CPE Mode Functions

5.1 External Network Connection

5.1.1 Network Requirement

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE mode, APO1000/APO1010 is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to APO1000/APO1010 are in **different** subnet from those connected to Main Base Station, and, in CPE mode, it **does not** accept wireless association from wireless clients.

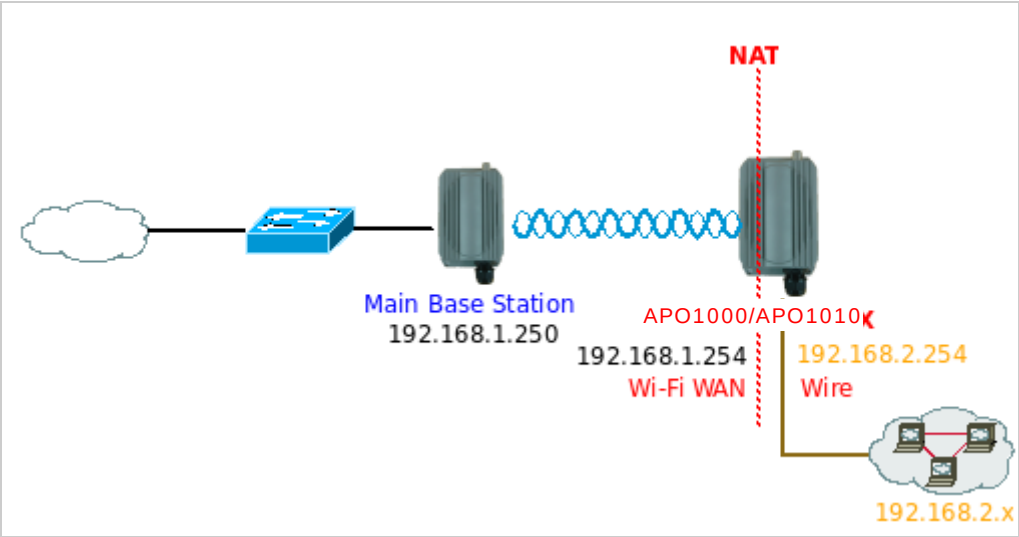
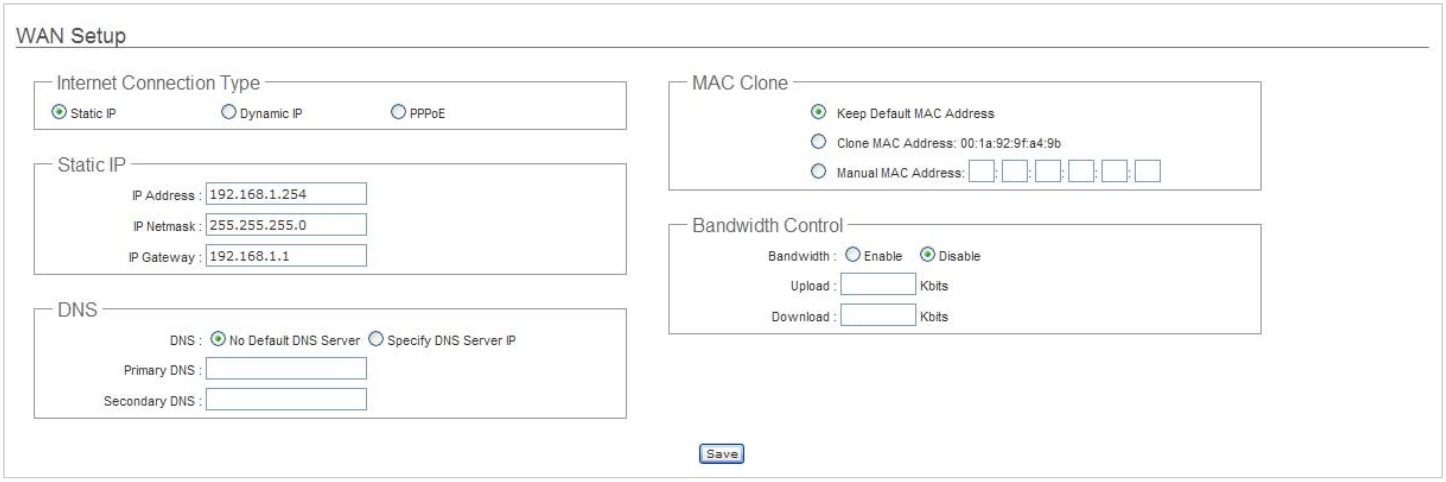


Figure 5-1 CPE mode configuration

5.1.2 Configure WAN Setup

There are three connection types for the WAN port : **Static IP**, **Dynamic IP** and **PPPoE**.

Please click on **System -> WAN** and follow the below setting.



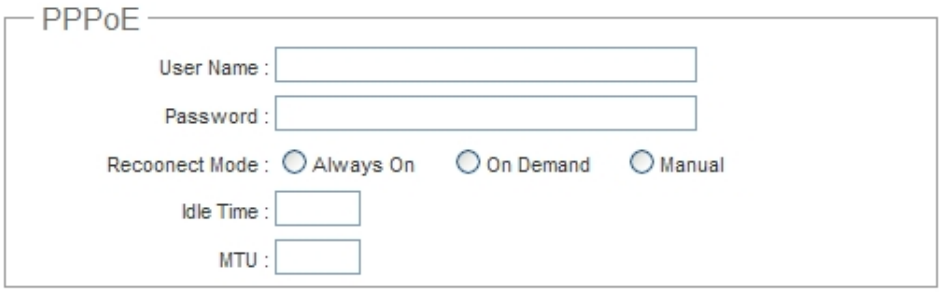
In CPE mode, the WAN Port is the Wireless interface.

- **Mode :** By default, it's "**Static *IP***". Check "Static IP", "Dynamic IP" or "PPPoE" to set up system WAN IP.
- **Static IP :** Users can manually setup the WAN IP address with a static IP provided by WISP.
  - ✓ **IP Address :** The IP address of the WAN port. By default, the IP address is 192.168.1.254
  - ✓ **IP Netmask :** The Subnet mask of the WAN port. By default, the Netmask is 255.255.255.0
  - ✓ **IP Gateway :** The default gateway of the WAN port. By default, the Gateway is 192.168.1.1

- **Dynamic IP :** Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings including DNS can be available from DHCP server. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click ***Release*** button to release IP address and click ***Renew*** button to renew IP address again.

  - ✓ **Hostname :** The Hostname of the WAN port

- **PPPoE :** To create wireless PPPoE WAN connection to a PPPoE server in network.



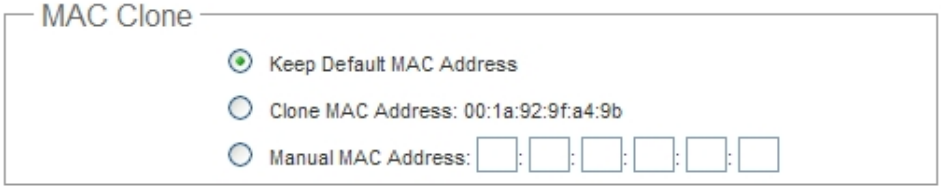
- ➔ **User Name :** Enter User Name for PPPoE connection
- ➔ **Password :** Enter Password for PPPoE connection
- ➔ **Reconnect Mode :**
  - ✓ **Always on** – A connection to Internet is always maintained.
  - ✓ **On Demand** – A connection to Internet is made as needed.

*When **Time Server** is enabled at the "On Demand" mode, the "Reconnect Mode" will turn out "Always on".*

  - ✓ **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.
- ➔ **Idle Time :** Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes.
- ➔ **MTU :** By default, it's **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.

- **DNS :** Check "No Default DNS Server" or "Specify DNS Server IP" radial button as desired to set up system DNS.
  - ➔ **Primary :** The IP address of the primary DNS server.
  - ➔ **Secondary :** The IP address of the secondary DNS server.

- **MAC Clone :** The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.

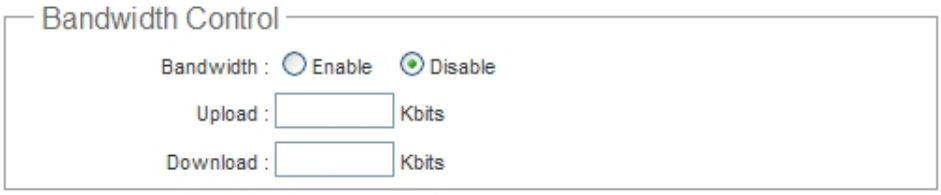


  - ➔ **Keep Default MAC Address :** Keep the default MAC address of WAN port on the system.
  - ➔ **Clone MAC Address :** If you want to clone the MAC address of the PC, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.

The Clone MAC Address field will display MAC address of the PC connected to system. Click "Save" button can make clone MAC effective.

➔ **Manual MAC Address :** Enter the MAC address registered with your ISP.

■ **Bandwidth :** Administrator can control download and upload bandwidth. Default is **Disable**



➔ **Upload :** The range is from **256** to **8192** in Kbits

➔ **Download** : The range is from **256** to **8192** in Kbits

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.1.3 Configure DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address.

Please click on **System -> DDNS Setup** and follow the below setting.

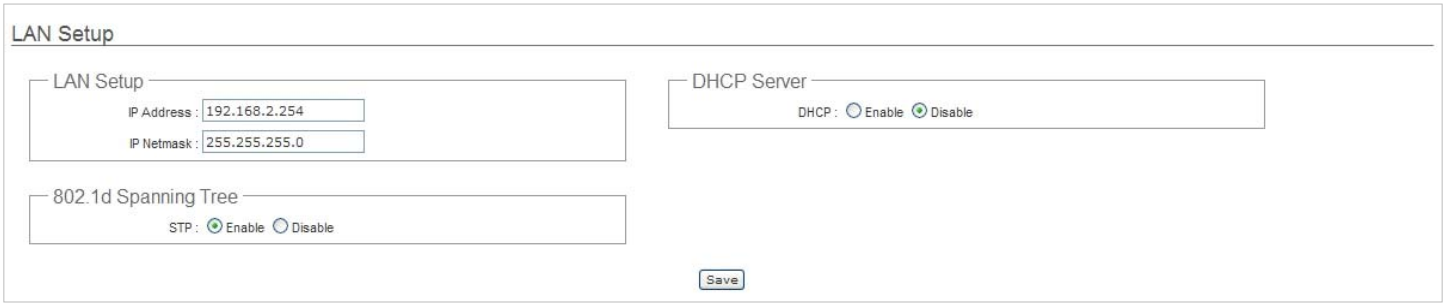
- **Enabled:** By default, it's "***Disable***". The mapping domain name won't change when dynamic IP changes. The beauty of it is no need to remember the dynamic WAP IP while accessing to it.
- **Service Provider:** Select the preferred Service Provider from the drop-down list including *dyndns*, *dhs*, *ods* and *tzo*
- **Hostname:** Host Name that you register to Dynamic-DNS service and export.
- **User Name & Password:** User Name and Password are used to login DDNS service.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.1.4 Configure LAN IP

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.

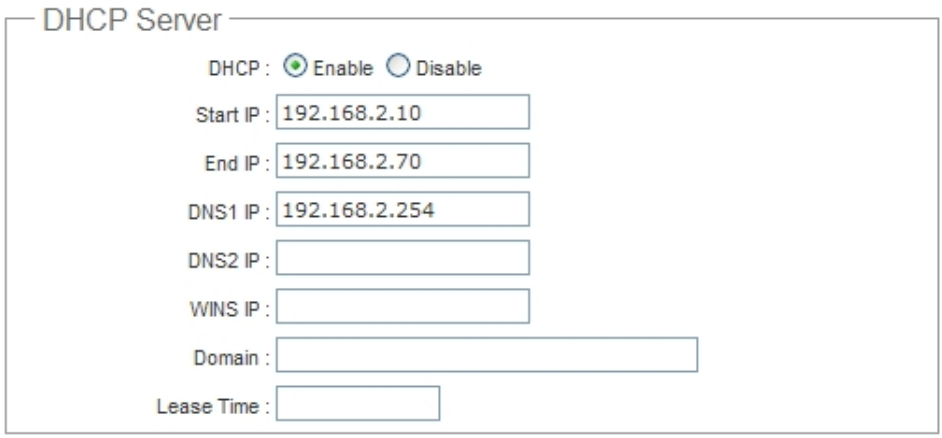


- **LAN IP :** The administrator can manually setup the LAN IP address.
  - ➔ **IP Address :** The IP address of the LAN port; default IP address is 192.168.10.100
  - ➔ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0

  - ➔ **802.1d Spanning Tree**

    The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

- **DHCP Server :** Devices connected to the system can obtain an IP address automatically when this service is enabled.



  - ➔ **DHCP :** Check ***Enable*** button to activate this function or ***Disable*** to deactivate this service.
  - ➔ **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.10.101 to 192.168.10.254, the netmask is 255.255.255.0
  - ➔ **DNS1 IP :** Enter IP address of the first DNS server; this field is required.

- ➔ **DNS2 IP :** Enter IP address of the second DNS server; this is optional.
- ➔ **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ➔ **Domain :** Enter the domain name for this network.
- ➔ **Lease Time :** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

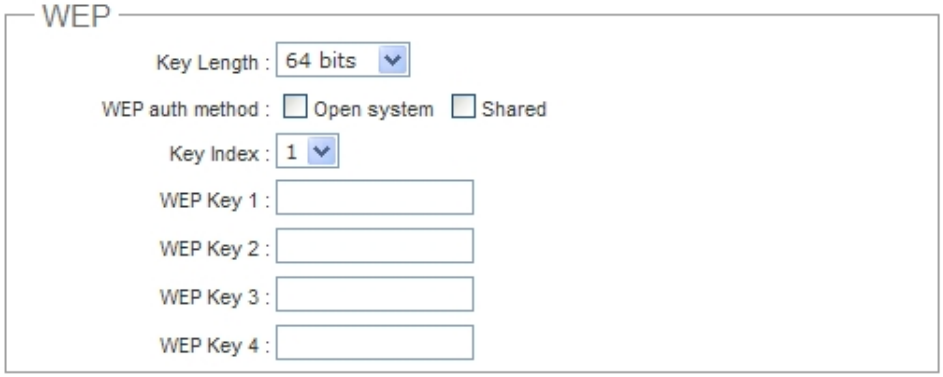
5.2 Access Point Association

5.2.1 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

- **ESSID :** Assign Service Set ID for the wireless system.
- **Band Mode :** Select an appropriate wireless band; bands available are 801.11b, 802.11g and 802.11b+802.11g.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from 1 to 54Mbps for 802.11g and 802.11b/g modes, or 1 to 11Mbps for 802.11b mode.
- **Country :** Select the desired Country code from the drop-down list; the options are US, ETSI or Japan.
- **Channel :** The channel range will be changed by selecting different country code. The channel range from 1 to 11 for US country code, or 1 to 13 for ETSI country code, or 1 to 14 for JP country code.
- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select the LEVEL 1 to LEVEL 9 you needed for your environment. If you are not sure of which setting to choose, then keep the default setting, LEVEL 9.
- **Security Type :** Select the desired security type from the drop-down list; the options are **Disabled WEP**, **WPA-PSK** and **WPA2-PSK**.

  ➔ **Disable :** Data are unencrypted during transmission when this option is selected.



  ➔ **WEP :** Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared

key. The WEP key configured here must be exactly the same as the key on the access point that this system is associated with.

- ✓ **Key Length :** The available options are ***64 bits***, ***128 bits*** or ***152 bits***.
- ✓ **WEP auth Method :** Enable the desired option among ***Open system*** and ***Shared***.
- ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters
152-bit	32 characters	16 characters

➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2)Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

- ✓ **Cipher Suite :** Select either AES or TKIP for the Cipher Suite.
- ✓ **Key Type :** Select either **ASCII** or **HEX** format for the Pre-shared Key.
- ✓ **Pre-shared Key :** Enter the pre-shared key; the format shall go with the selected key type.

Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

5.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

- **Slot Time :** Slot time is in the range of **1~1489** and set in unit of ***microsecond***. The default value is **20** microsecond.

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **48** microsecond.

  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughputs become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor

performance the ACK Timeout could be made longer to accommodate.

RTS/CTS

Adjustment of RTS Threshold can be done to turn on RTS. CTS Timeout will take effect only when RTS is turned on.

Unlike wired Ethernet, radio transmission may begin with a RTS (Request to Send) frame, and receiver responds with a CTS (Clear to Send) frame. The RTS/CTS mechanism is called *Channel Cleaning*, all stations that received CTS will back off for certain period of time, multiple of the slot time.

Each CTS packet has a NAV (Network Allocation Vector) number n, the channel is reserved for sender and receiver for additional *n-millisecond*. The NAV guarantees the channel is free of interference in next n-millisecond. The last packet of ACK will set NAV to zero, indicated that connection is done and free the channel to others.

- **CTS Timeout :** CTS Timeout is in the range of **1~744** and set in unit of ***microsecond***. The default value is **48** microsecond.

  CTS Timeout will take effect only when RTS is turned on. Adjustment of RTS Threshold can be done to turn on RTS. When hidden wireless stations are present in the wireless network RTS can be considered to turn on to minimize collisions and increase performance. Ensure CTS timeout is long enough to avoid frequent re-transmission of RTS.

Slot Time and ACK/CTS Timeout settings for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256**~**2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** RTS Threshold is in the range of **1~2346** byte. The default is **2346** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

  With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **WMM :** By default, it's "***Disable***".

Select “Enable”, then packets with WMM QoS will take higher priority.

WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. Packets with QoS header including Diffserv/IP ToS and 802.1p will be mapped into 4 Access Categories of WMM, packets without QoS header will be assigned to the Best Effort queue. Please refer to the table below for mapping from 802.1p and ToS mapping to WMM:

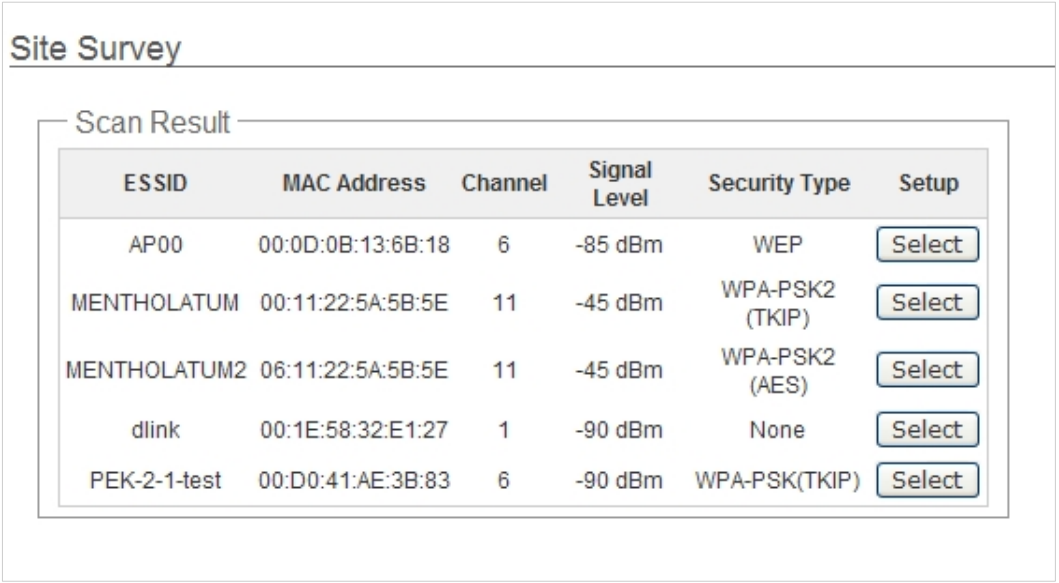
Queue	Data Transmitted Clients to AP	IP ToS	802.1P Priority	Priority	Description
AC_BK	Background.	0x08 0x20	1, 2	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort		0, 3	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	0x28 0xa0	4, 5	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	0x30 0xe0 0x88 0xb8	6, 7	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to all VAPs.

5.2.3 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.



- **ESSID : Available** Extend Service Set ID of surrounding Access Points.
- **MAC Address :** MAC addresses of surrounding Access Points.
- **Channel :** Channel numbers used by all found Access Points.
- **Signal Level :** Received signal strength of all found Access Points.
- **Security Type :** Security type by all found Access Points.
- **Setup :** Click "**Select**" button to configure settings and associate with chosen AP.

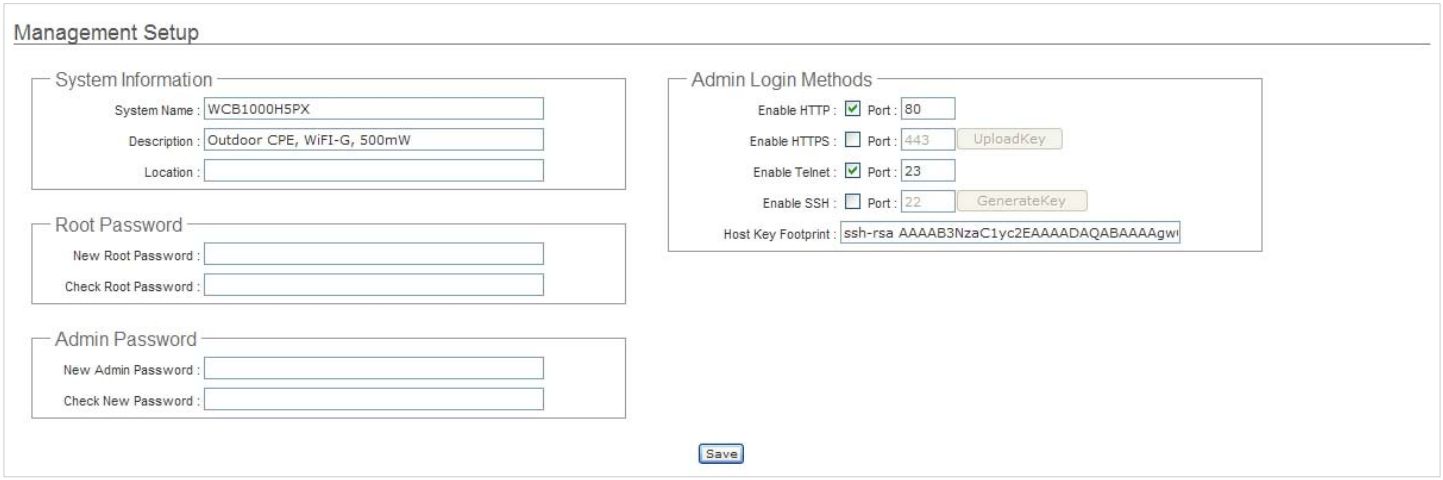
*While clicking "Select" button in the Site Survey Table, the "**ESSID**" and "**Security Type**" will apply in the Wireless General Setup. However, more settings are needed including Security Key.*

5.3 System Management

5.3.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.



- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default one.
  - ➔ **Description :** Provide description of the system.
  - ➔ **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to ***Appendix C. Network manager Privileges***.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only **root** user can enable or disable system login methods and change services port.
  - ➔ **Enable HTTP :** Check to select HTTP Service.
  - ➔ **HTTP Port :** The default is **80** and the range is between 1 ~ 65535.
  - ➔ **Enable HTTPS :** Check to select HTTPS Service
  - ➔ **HTTPS Port :** The default is **443** and the range is between 1 ~ 65535.

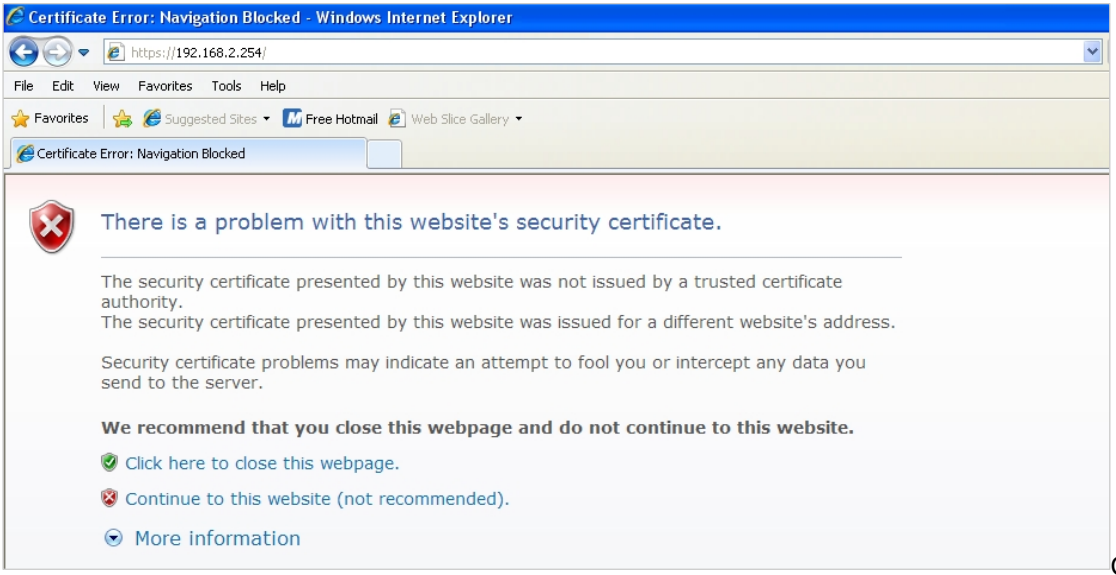
*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

  - ➔ **Enable Telnet :** Check to select Telnet Service
  - ➔ **Telnet Port :** The default is **23** and the range is between 1 ~ 65535.
  - ➔ **Enable SSH :** Check to select SSH Service
  - ➔ **SSH Port :** Please The default is **22** and the range is between 1 ~ 65535.

*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's Web GUI (https://192.168.2.254). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click "***Continue to this website***" to access the system's Web GUI. The system's Overview page will appear.

5.3.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

- **Local Time :** Display the current system time.

- **NTP Client :** To synchronize the system time with NTP server.
  - ➔ **Enable :** Check to select NTP client.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time :** Enable or disable Daylight saving.

If the system time from NTS server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

5.3.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

- **UPnP :** By default, it's "***Disable***". Select "**Enable**" or "***Disable"*** of UPnP Service.

  Click ***Save*** button to save changes and click ***Reboot*** button to activate changes

For UPnP to work in Windows XP, the "APO1000" or "APO1010" must be available in "***My Network Places***".

If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to ***Appendix D. Using UPnP on Windows XP***

5.3.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

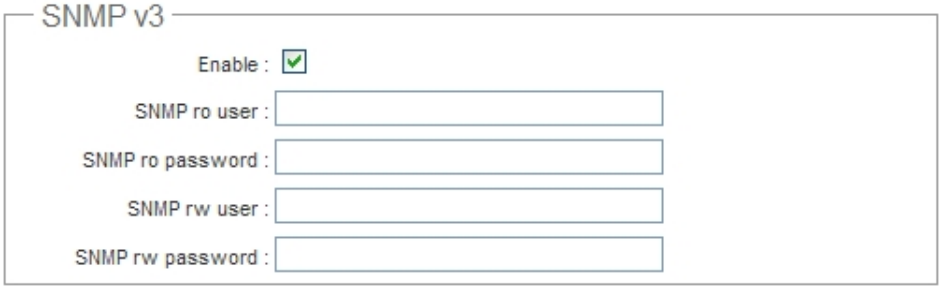
Please click on **System -> SNMP Setup** and follow the below setting.

- **SNMP v2c Enable:** Check to enable SNMP v2c.

  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

  SNMPv3 supports the highest level SNMP security.



  - ➔ **SNMP ro user :** Set a community string to authorize read-only access.
  - ➔ **SNMP ro password :** Set a password to authorize read-only access.
  - ➔ **SNMP rw user :** Set a community string to authorize read/write access.
  - ➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

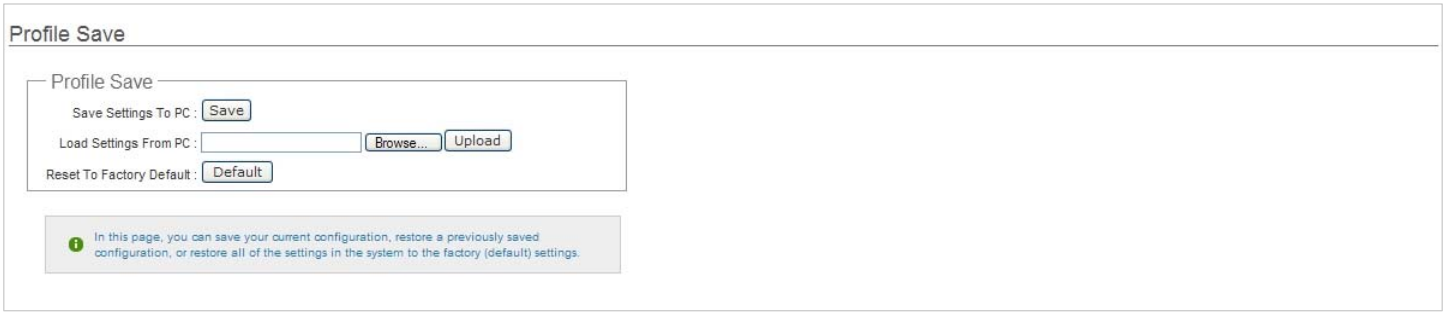
  - ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
  - ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

Click ***Save*** button to save changes and click ***Reboot*** button to activate.

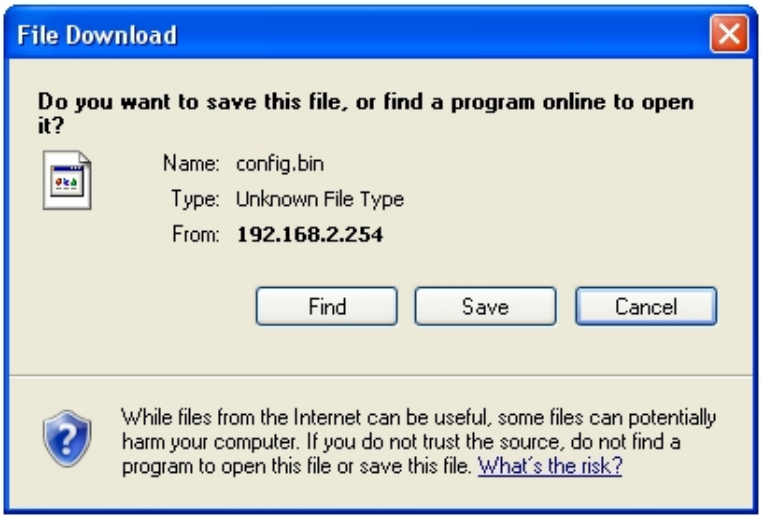
5.3.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.



- **Save Settings to PC :** Click ***Save*** button to save the current configuration to a local disk.

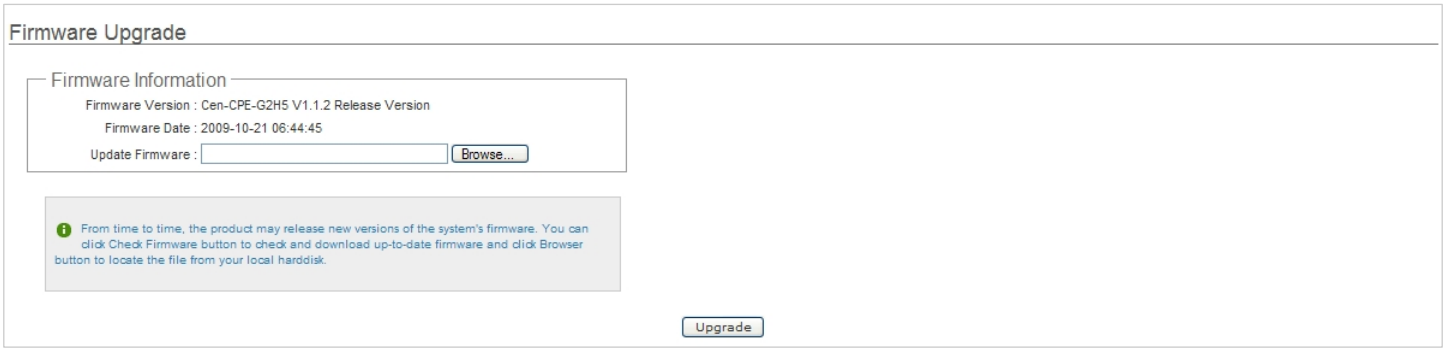


- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

5.3.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **8 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.

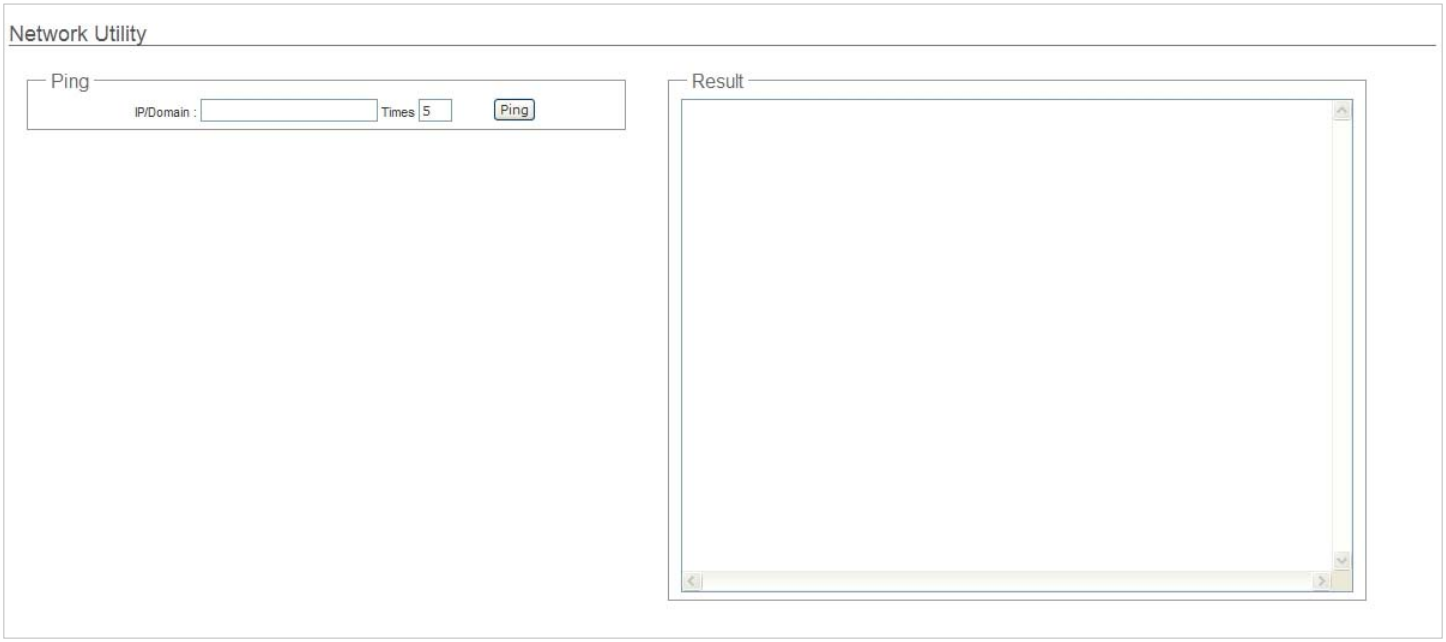


1. *To prevent data loss during firmware upgrade, please back up current settings before proceeding.*
2. *Do not interrupt during firmware upgrade including power on/off as this may damage system.*

5.3.7 Network Utility

The administrator can diagnose network connectivity via the PING utility.

Please click on **Utilities -> Network Utility** and follow the below setting.

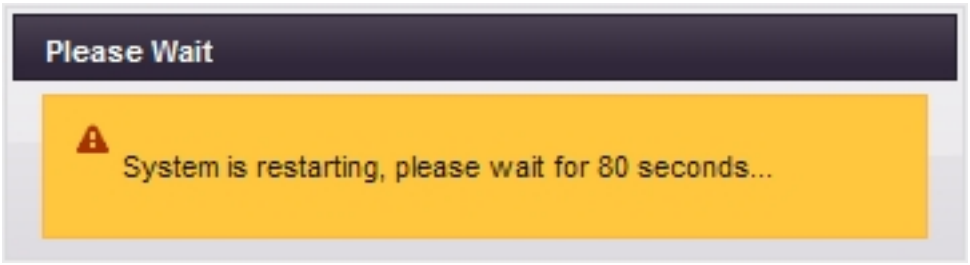


- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count :** By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

5.3.8 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



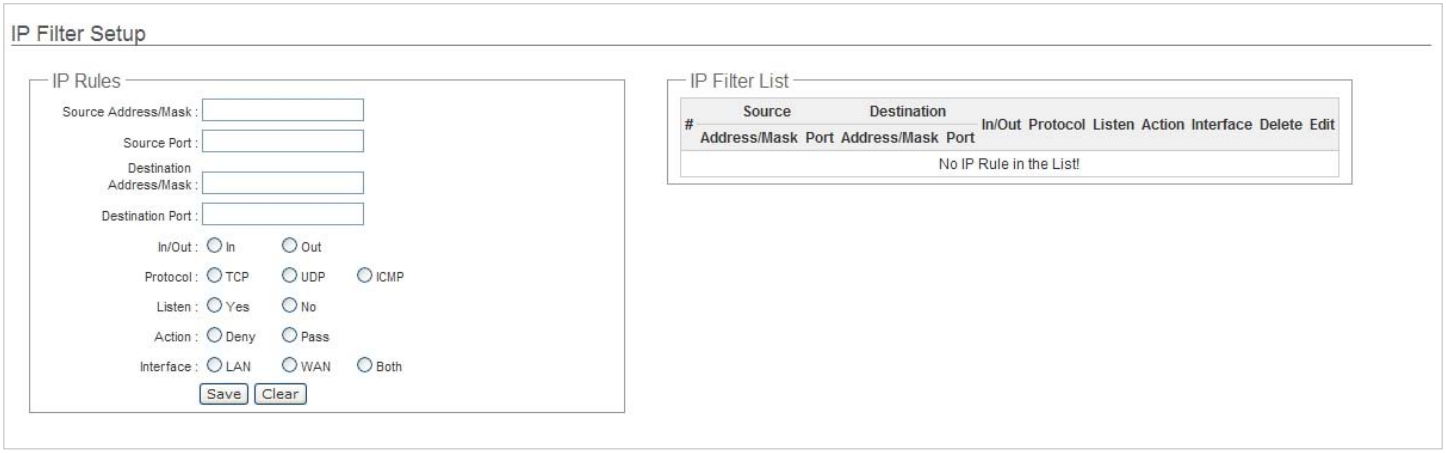
The **System Overview** page appears upon the completion of reboot.

5.4 Access Control List

5.4.1 IP Filter Setup

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

Please click on **Advance -> IP Filter Setup** and follow the below setting.



- **Source Address/Mask :** Enter desired source IP address and netmask; i.e. 192.168.2.10/32.
- **Source Port :** Enter a port or a range of ports as ***start:end***; i.e. port 20:80
- **Destination Address/Mask :** Enter desired destination IP address and netmask; i.e. 192.168.1.10/32
- **Destination Port :** Enter a port or a range of ports as ***start:end***; i.e. port 20:80
- **In/Out :** Applies to Ingress or egress packets
- **Protocol :** Supports ***TCP***, ***UDP*** or ***ICMP***.
- **Listen :** Click ***Yes*** radial button to match TCP packets only with the SYN flag.
- **Active :** ***Deny*** to drop and ***Pass*** to allow per filter rules
- **Interface :** The interface that a filter rule applies

All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Click “**Save**” button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

- **Example 1 :** Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.2/32		192.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN

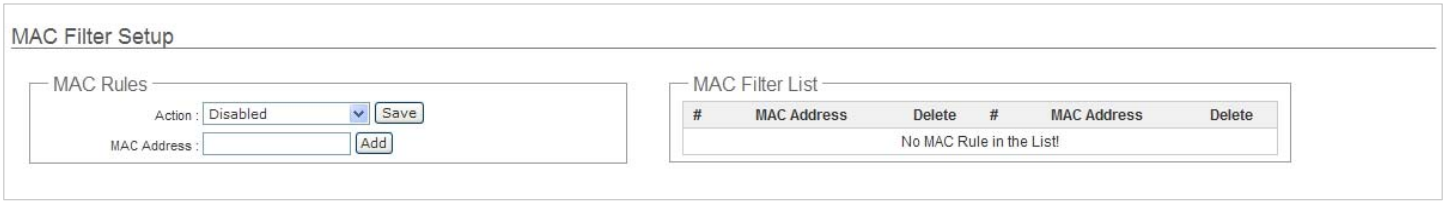
- **Example 2 :** All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN
2	192.168.2.2/32		192.2.254/32	22	In	TCP	n	pass	LAN

5.4.2 MAC Filter Setup

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important to note that MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.



- **MAC Filter Rule :** By default, it's "***Disable***". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click ***Save*** button to save your change.

  Two ways to set the Access Control List:

  ➔ **Only Allow List MAC**.

  The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

  ➔ **Only Deny List MAC**.

  The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.

- **MAC Address :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons***.***

Click ***Reboot*** button to activate your changes

5.5 Resource Sharing

5.5.1 DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.

Please click on **Advance -> DMZ** and follow the below setting.

- **DMZ :** By default, it's "***Disable***". Check ***Enable*** radial button to enable DMZ.
- **IP Address :** Enter IP address of DMZ host and only one DMZ host is supported.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes.

5.5.2 Virtual Server (Port Forwarding)

"Virtual Server" can also referred to as "Port Forward" as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Please click on **Advance -> Virtual Server** and follow the below setting.

- **Virtual Server :** By Default, It's "***Disable***"***.*** Check ***Enable*** radial button to enable Virtual Server.
- **Description :** Enter appropriate message for resource sharing via Virtual Server.
- **Private IP :** Enter corresponding IP address of internal resource to share.
- **Protocol Type :** Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80
- **Public Port :** A port or a range of ports may be specified as ***start:end***; i.e. port 20:80

The Private Port and Public Port can be different. However, total number of ports need to be the same.
Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.

Click "**Add**" button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes. While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

- **Example 1 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP ***20~80*** will be redirected to port TCP ***20~80*** of ***192.168.2.11***

DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.10	22	22
2	TCP	192.168.2.11	20:80	20:80

- **Example 2 :** All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port ***20~80*** will be redirected to port ***20~80*** of ***192.168.2.11***. The rule 2 won't take effect.

DMZ Enabled : 192.168.2.12

Rule	Protocol	Private IP	Private Port	Public Port
1	TCP	192.168.2.11	20:80	20:80
2	TCP	192.168.2.10	22	22

5.6 System Status

This section breaks down into subsections of ***System Overview***, ***DHCP Clients***, ***Extra Information*** and ***Event Log***.

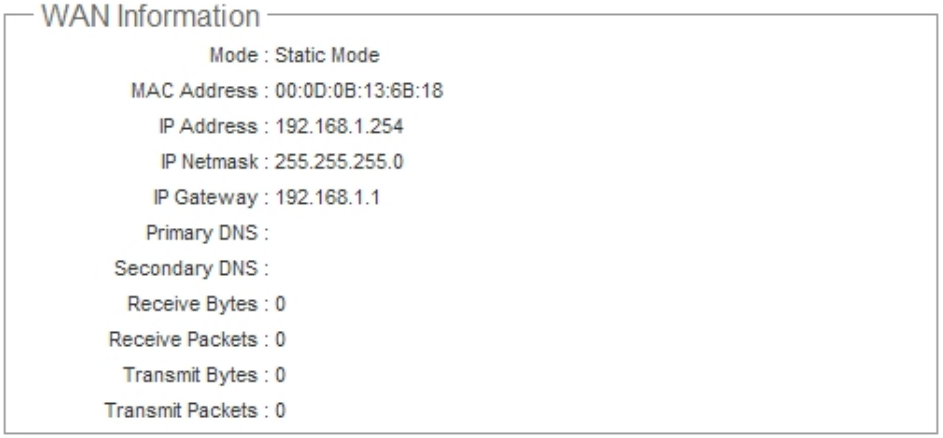
5.6.1 System Overview

Detailed information on **System**, **WAN Information**, **LAN Information** and **Wireless Station Information** can be reviewed via this page.

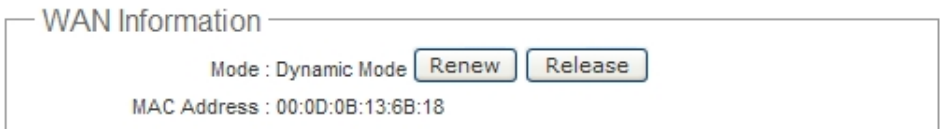
- **System :** Display the information of the system.

  - ➔ **System Name :** The name of the system.
  - ➔ **Operating Mode :** The mode currently in service.
  - ➔ **Location :** The reminding note on the geographical location of the system.
  - ➔ **Description :** The reminding note of the system.
  - ➔ **Firmware Version :** The current firmware version installed.
  - ➔ **Firmware Date :** The build time of the firmware installed.
  - ➔ **Device Time :** The current time of the system.
  - ➔ **System Up Time :** The time period that system has been in service since last reboot.

- **WAN Information :** Display the information of the WAN interface.



The WAN port specified **Dynamic IP**, the Release and Renew button will be show-up, click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.



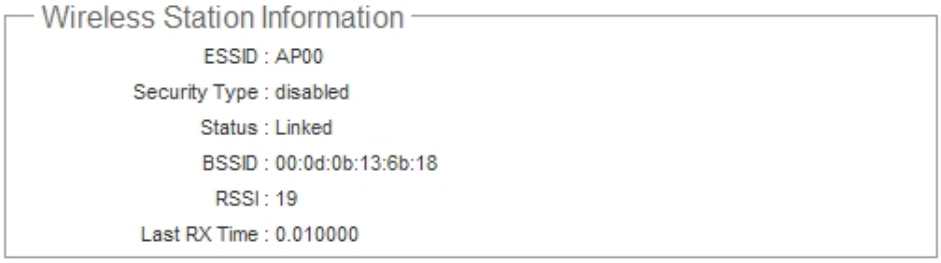
The WAN port specified **PPPoE**, and the **Connect** and **DisConnect** button will be show up. Click "**Connect**" button to assigned IP address from PPPoE server, "**DisConnect**" button to release IP address of WAN port.

- ➔ **Mode :** Supports Static, Dynamic, and PPPoE modes.
- ➔ **Reconnect Mode :** The current reconnect mode of the PPPoE.
- ➔ **MAC Address :** The MAC address of the WAN port.
- ➔ **IP Address :** The IP address of the WAN port.
- ➔ **IP Netmask :** The IP netmask of the WAN port.
- ➔ **IP Gateway :** The gateway IP address of the WAN port.
- ➔ **Primary DNS :** The primary DNS server in service.
- ➔ **Secondary DNS :** The secondary DNS server in service.
- ➔ **Receive bytes :** The total received packets in bytes on the WAN port.
- ➔ **Receive packets :** The total received packets of the WAN port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes of the WAN port.
- ➔ **Transmit packets :** The total transmitted packets of the WAN port.

- **Wireless Station Information :** Display the information of the associated AP.

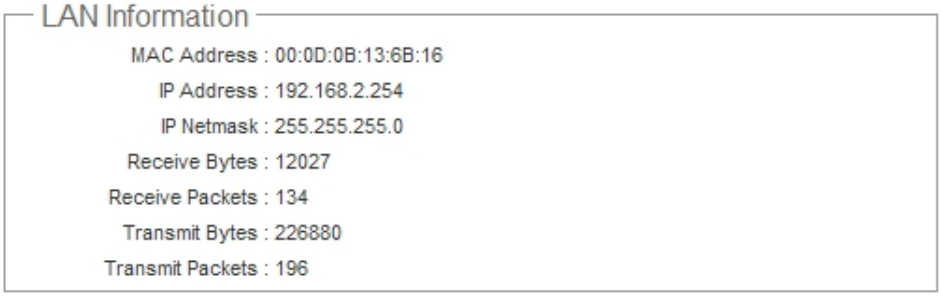
- ➔ **ESSID :** Display Extended Service Set ID of the associated AP currently.
- ➔ **Security :** Display security type of the associated AP currently.
- ➔ **Status :** Display connection status of the associated AP currently.

If the system associate with AP, the BSSID, RSSI and Last Rx Time will be show up. Below depicts the examples for associated AP of Wireless Information.



- ➔ **BSSID :** Indicate the Basic Service Set ID of the associated AP
- ➔ **RSSI :** Indicate the RSSI of the associated AP.
- ➔ **Last Rx Time :** Indicate the last receive packet of the associated AP

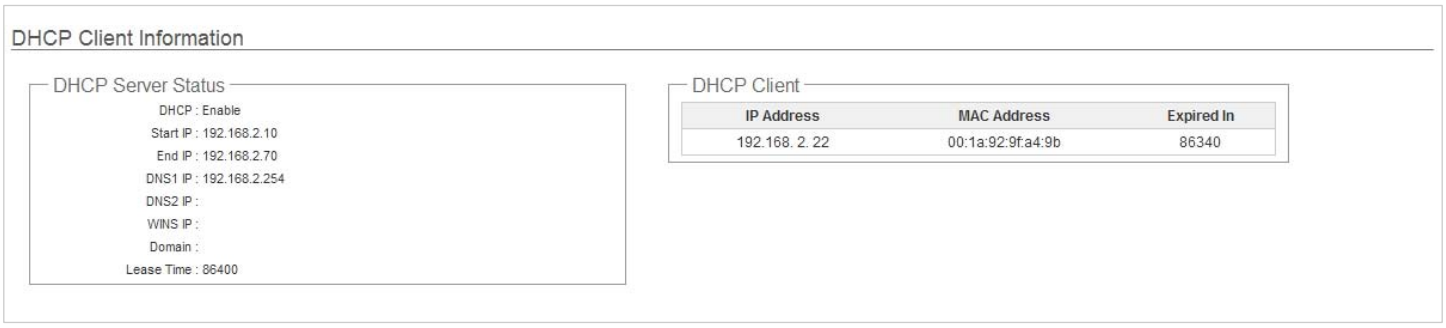
- **LAN Information :** Display total received and transmitted statistics on the LAN interface.



- ➔ **MAC Address :** The MAC address of the LAN port.
- ➔ **IP Address :** The IP address of the LAN port.
- ➔ **IP Netmask :** The IP netmask of the LAN port.
- ➔ **Receive bytes :** The total received packets in bytes on the LAN port.
- ➔ **Receive packets :** The total received packets of the LAN port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes of the LAN port.
- ➔ **Transmit packets :** The total transmitted packets of the LAN port.

5.6.2 DHCP Clients

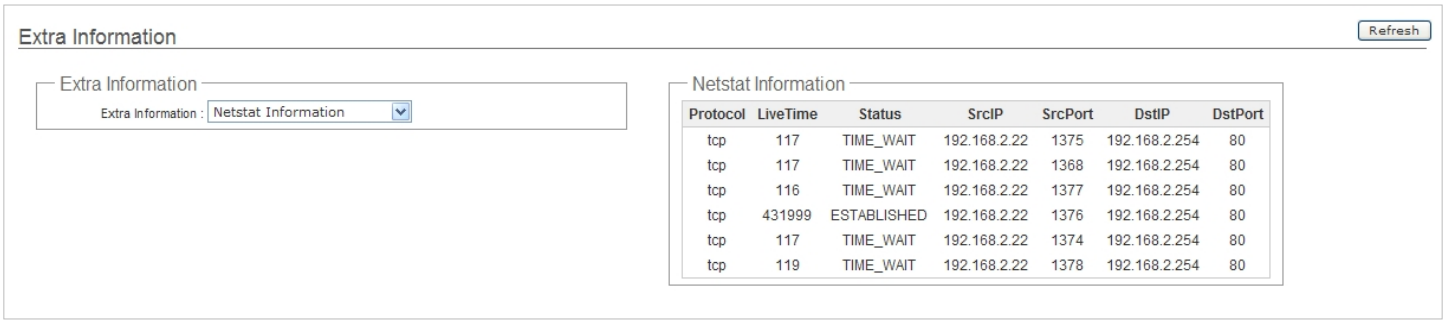
Users could retrieve DHCP server and DHCP clients' IP/MAC address via this page.



- **IP address :** IP addresses to LAN devices by DHCP server.
- **MAC Address :** MAC addresses of LAN devices.
- **Expired In :** Shows how long the leased IP address will expire.

5.6.3 Extra Info

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

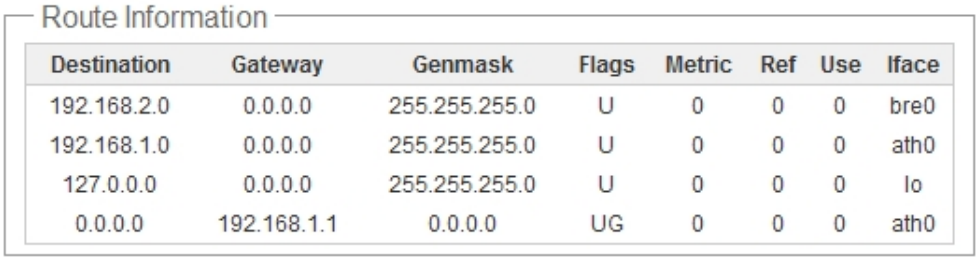


- **Netstat Information :** Select “**NetStatus Information**” on the drop-down list, the connection track list should show-up, the list can be updated using the Refresh button.

  NetStatus will show all connection track on the system, the information include *Protocol*, *Live Time*, *Status* , *Source/Destination IP address* and *Port*.

- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

  APO1000/APO1010 could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.



- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

  ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

  Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces.

Bridge Table Information

Bridge Port	Bridge ID	STP Enabled	Interface
bre0	8000.000d0b136b16	yes	eth0

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

  This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

  Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.

Bridge MACs Information

Port No	MAC Address	Local	Ageing Timer
1	00:0d:0b:13:6b:16	yes	0.00
1	00:1a:92:9f:a4:9b	no	0.05

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.

Bridge STP Information

bre0			
bridge id	8000.000d0b136b16		
designated root	8000.000d0b136b16		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00	gc interval	0.00
hello timer	0.71	tcn timer	0.00
topology change timer	0.00	gc timer	1.71
flags			

eth0 (1)			
port id	8001	state	forwarding
designated root	8000.000d0b136b16	path cost	100
designated bridge	8000.000d0b136b16	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.00
flags			

5.6.4 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as troubleshooting tool when issues are experienced in system.

- **Time:** The date and time when the event occurred.
- **Facility:** It helps users to identify source of events such “System” or “User”
- **Severity:** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message:** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

Chapter 6. Client Bridge + Universal Repeater Configuration

When Client Bridge + Universal Repeater mode is activated, the system can be configured as an **Access Point** and **Client Station** simultaneously. This section provides information in configuring the Client Bridge + Universal Repeater mode with graphical illustrations. APO1000/APO1010 provides functions as stated below where they can be configured via a user-friendly web based interface.

Option	System	Wireless	Utilities	Status
Functions	Operating Mode	General Setup	Profiles Settings	System Overview
	LAN	Advanced Setup	Firmware Upgrade	Clients
	Management	AP Setup	Network Utility	DHCP Clients
	Time Server	MAC FIlter	Reboot	Extra Info
	SNMP	Site Survey		Event Log
	UPNP			

Table 6-1: Client Bridge + Universal Repeater Mode Functions

6.1 External Network Connection

6.1.1 Network Requirement

It can be used as an Client Bridge or Universal Repeater to receive wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, APO1000/APO1010 is enabled with DHCP Server functions. The wired clients of APO1000/APO1010 are in **the same** subnet from Main Base Station and it **accepts** wireless connections from client devices.

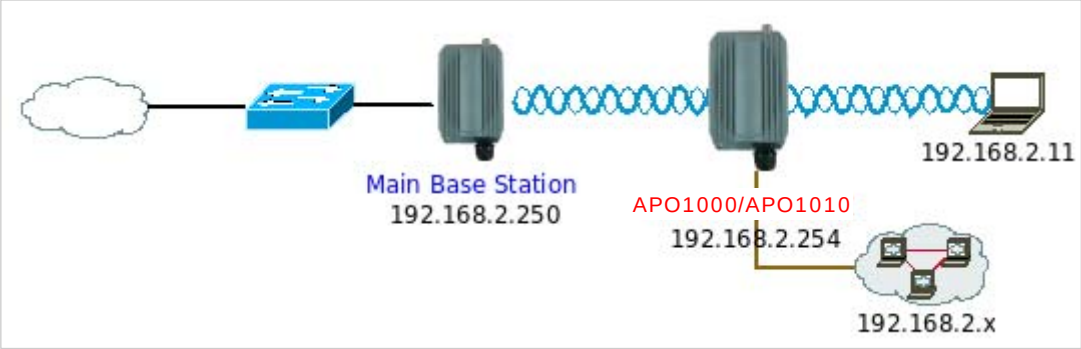


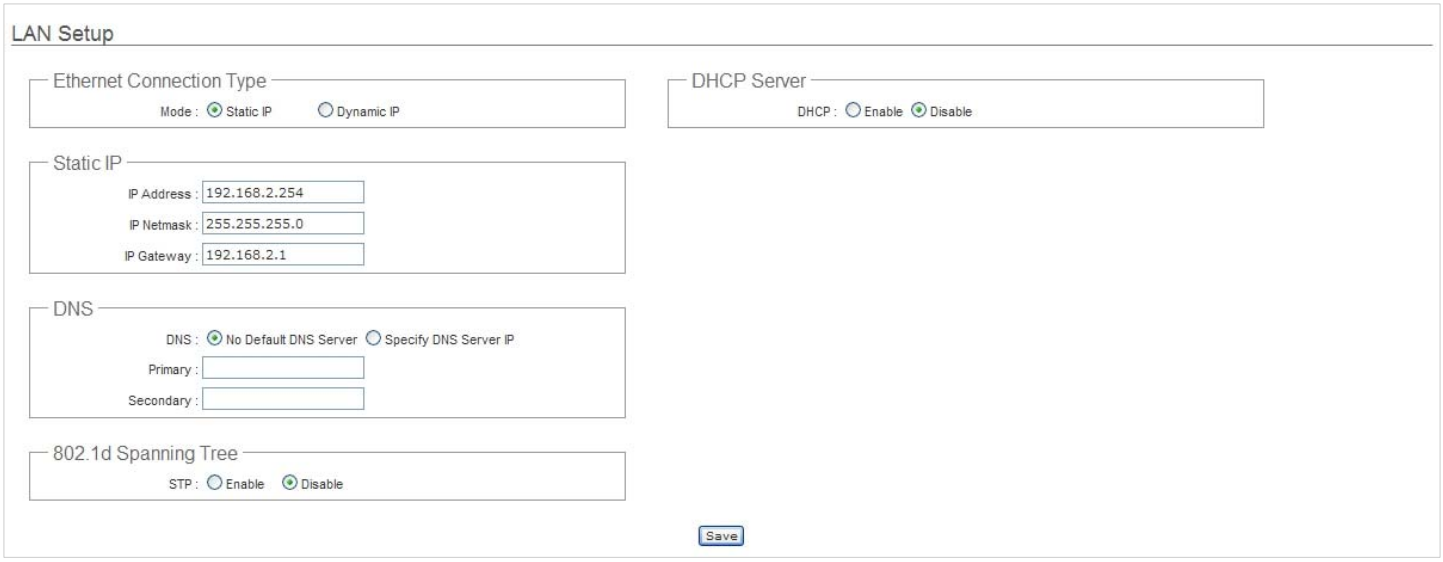
Figure 6-1 Client Bridge + Universal Repeater mode Configuration

When the APO1000/APO1010 configured as an Access Point and Client Station simultaneously, the Wireless General and Advanced Setup also used simultaneously. But the Security Type can be different. In the other word, the channel or other settings will be the same between APO1000/APO1010 to Main Base Station and wireless client to APO1000/APO1010, but security type can be different.

6.1.2 Configure LAN IP

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.



- **Mode :** Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
  - ➔ **Static IP :** The administrator can manually setup the LAN IP address when static IP is available/ preferred.
    - ✓ **IP Address :** The IP address of the LAN port; default IP address is 192.168.2.254
    - ✓ **IP Netmask :** The Subnet mask of the LAN port; default Netmask is 255.255.255.0
    - ✓ **IP Gateway :** The default gateway of the LAN port; default Gateway is 192.168.2.1
  - ➔ **Dynamic IP :** This configuration type is applicable when the APO1000/APO1010 is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

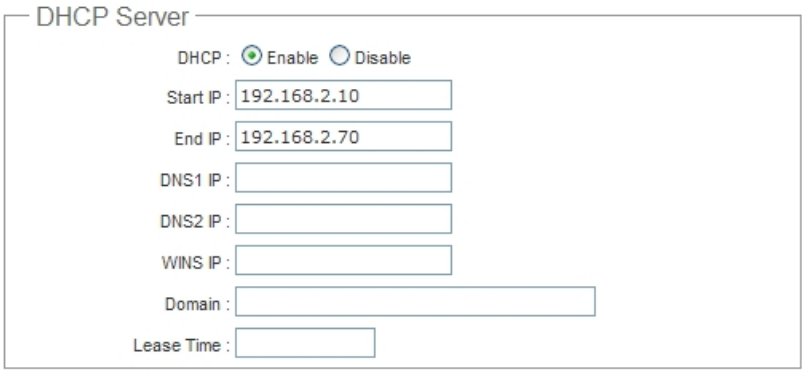
    - ✓ **Hostname :** The Hostname of the LAN port

- **DNS :** Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
  - ➔ **Primary :** The IP address of the primary DNS server.
  - ➔ **Secondary :** The IP address of the secondary DNS server.

- **802.1d Spanning Tree**

  The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

- **DHCP Setup :** Devices connected to the system can obtain an IP address automatically when this service is enabled.



  - ➔ **DHCP :** Check ***Enable*** button to activate this function or ***Disable*** to deactivate this service.
  - ➔ **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
  - ➔ **DNS1 IP :** Enter IP address of the first DNS server; this field is required.
  - ➔ **DNS2 IP :** Enter IP address of the second DNS server; this is optional.
  - ➔ **WINS IP :** Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
  - ➔ **Domain :** Enter the domain name for this network.
  - ➔ **Lease Time :** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

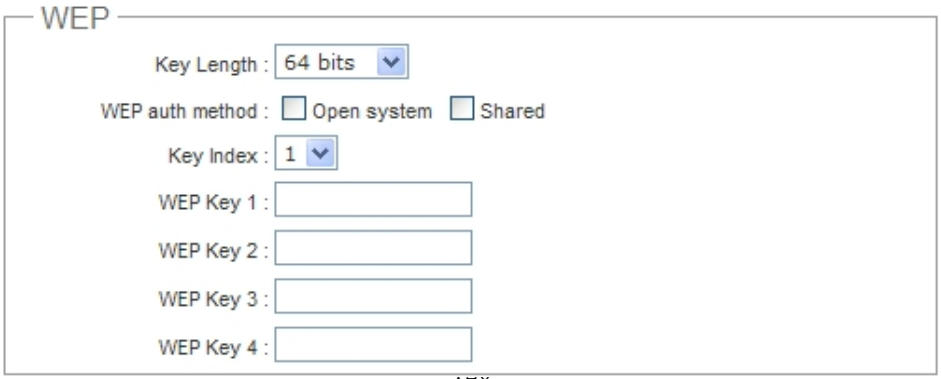
Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

6.2 Access Point Association

6.2.1 Configure Wireless General Setting

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

- **ESSID :** Assign Service Set ID for the wireless system.
- **Band Mode :** Select an appropriate wireless band; bands available are 801.11b, 802.11g and 802.11b+802.11g.
- **Transmit Rate Control :** Select the desired rate from the drop-down list; the options are auto or ranging from 1 to 54Mbps for 802.11g and 802.11b/g modes, or 1 to 11Mbps for 802.11b mode.
- **Country :** Select the desired Country code from the drop-down list; the options are US, ETSI or Japan.
- **Channel :** The channel range will be changed by selecting different country code. The channel range from 1 to 11 for US country code, or 1 to 13 for ETSI country code, or 1 to 14 for JP country code.
- **Tx Power :** You can adjust the output power of the system to get the appropriate coverage for your wireless network. Select the LEVEL 1 to LEVEL 9 you needed for your environment. If you are not sure of which setting to choose, then keep the default setting, LEVEL 9.
- **Security Type :** Select the desired security type from the drop-down list; the options are **Disabled WEP**, **WPA-PSK** and **WPA2-PSK**.
  - ➔ **Disable :** Data are unencrypted during transmission when this option is selected.
  - ➔ **WEP :** Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key. The WEP key configured here must be exactly the same as the key on the access point that this system is associated with.



- ✓ **Key Length :** The available options are ***64 bits***, ***128 bits*** or ***152 bits***.
- ✓ **WEP auth Method :** Enable the desired option among ***Open system*** and ***Shared***.
- ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters
152-bit	32 characters	16 characters

➔ **WPA-PSK (or WPA2-PSK) :** WPA (or WPA2)Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

- ✓ **Cipher Suite :** Select either AES or TKIP for the Cipher Suite.
- ✓ **Key Type :** Select either **ASCII** or **HEX** format for the Pre-shared Key.
- ✓ **Pre-shared Key :** Enter the pre-shared key; the format shall go with the selected key type.

Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **Station** and **Repeater AP**. The "**Security Type**" settking will be applied to **Station**.

6.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

- **Slot Time :** Slot time is in the range of **1~1489** and set in unit of ***microsecond***. The default value is **20** microsecond.

  Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **ACK Timeout :** ACK timeout is in the range of **1~372** and set in unit of ***microsecond***. The default value is **48** microsecond.

  All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout".

  ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packet before ACK is received, and throughputs become low due to excessively high re-transmission.

  ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.

RTS/CTS

Adjustment of RTS Threshold can be done to turn on RTS. CTS Timeout will take effect only when RTS is turned on.

Unlike wired Ethernet, radio transmission may begin with a RTS (Request to Send) frame, and receiver responds with a CTS (Clear to Send) frame. The RTS/CTS mechanism is called *Channel Cleaning*, all stations that received CTS will back off for certain period of time, multiple of the slot time.

Each CTS packet has a NAV (Network Allocation Vector) number n, the channel is reserved for sender and receiver for additional *n-millisecond*. The NAV guarantees the channel is free of interference in next n-millisecond. The last packet of ACK will set NAV to zero, indicated that connection is done and free the channel to others.

- **CTS Timeout :** CTS Timeout is in the range of **1~744** and set in unit of ***microsecond***. The default value is **48** microsecond.

  CTS Timeout will take effect only when RTS is turned on. Adjustment of RTS Threshold can be done to turn on RTS. When hidden wireless stations are present in the wireless network RTS can be considered to turn on to minimize collisions and increase performance. Ensure CTS timeout is long enough to avoid frequent re-transmission of RTS.

Slot Time and ACK/CTS Timeout settings for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **RSSI Threshold :** RSSI Threshold is in the range of **-128~127**.The default value is **24**.

  RSSI is defined as *Received Signal Strength Indication*, when the received signal strength from peer is below this threshold, the peer will be consider as disconnected. Set the threshold higher will make roaming happen earlier, set lower will allow weak signal peer to connect. In normal situation, the longer distance the lower signal strength will be sensed between peers people could consider to lower RSSI threshold to have bigger coverage from the AP or AP client perspective. If it doesn't work well then people could consider to jack up RSSI threshold to have stable smaller coverage and leave AP clients in longer distance to associate with closer AP.

- **Beacon Interval :** Beacon Interval is in the range of **1~5000** and set in unit of ***millisecond***. The default value is **100** msec.

  Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

  All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

  By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval :** The DTIM interval is in the range of **1**~**15**. The default is **15**.

  DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power

saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold :** The Fragment Threshold is in the range of **256**~**2346** byte. The default is **2346** byte.

  Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

  Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold :** RTS Threshold is in the range of **1~2346** byte. The default is **2346** byte.

  The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble :** By default, it's "***Enable***". To ***Disable*** is to use Long 128-bit Preamble Synchronization field.

  The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst :** By default, it's "***Enable***". To ***Disable*** is to deactivate Tx Burst.

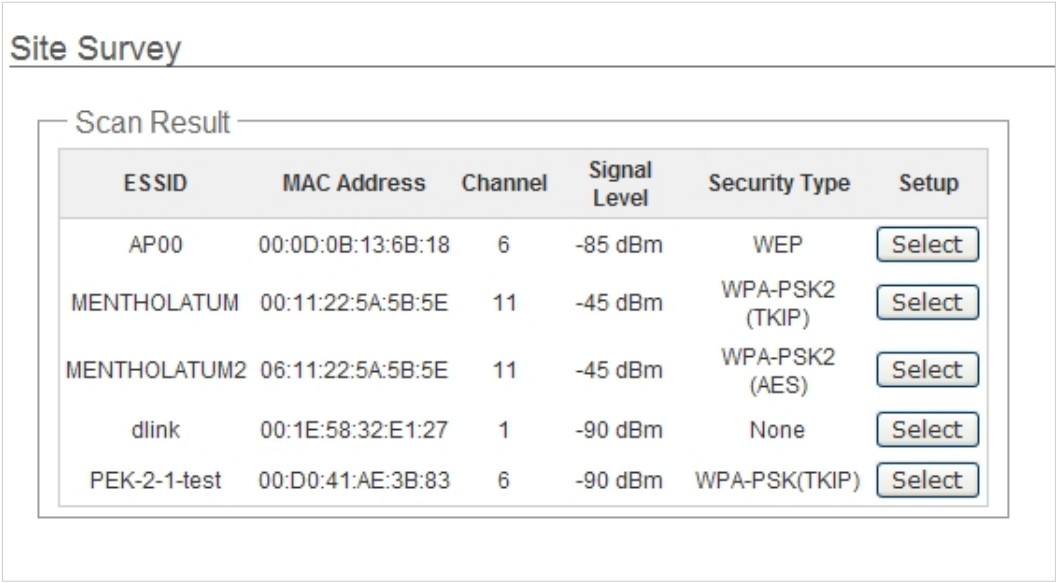
  With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

Change these settings as described here and click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **Station** and **Repeater AP**.

6.2.3 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.



- **ESSID : Available** Extend Service Set ID of surrounding Access Points.
- **MAC Address :** MAC addresses of surrounding Access Points.
- **Channel :** Channel numbers used by all found Access Points.
- **Signal Level :** Received signal strength of all found Access Points.
- **Security Type :** Security type by all found Access Points.
- **Setup :** Click "**Select**" button to configure settings and associate with chosen AP.

*While clicking "Select" button in the Site Survey Table, the "**ESSID**" and "**Security Type**" will apply in the Wireless General Setup. However, more settings are needed including Security Key.*

6.3 Wireless LAN Network Creation

The network manager can configure related wireless settings, **AP Setup, Security Settings,** and **MAC Filter Settings**.

6.3.1 AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings.

- **ESSID :** Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP clients associated with the specified repeater AP.
- **Enable AP :** By default, it's "***Enable***" repeater AP.

  Select "Enable" to activate repeater AP or click "Disable" to deactivate this function
- **Hidden SSID :** By default, it's "***Disable***".

  Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.
- **Client Isolation :** By default, it's "***Disable***".

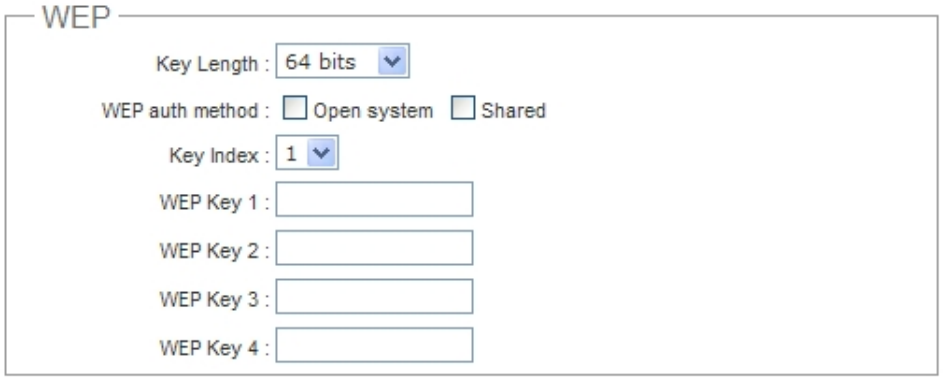
  Select "**Enable"**, all clients will be isolated from each other, which means they can't reach each other.
- **WMM :** By default, it's "***Disable***"***.***

  Select "Enable", then packets with WMM QoS will take higher priority.

  WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. Packets with QoS header including Diffserv/IP ToS and 802.1p will be mapped into 4 Access Categories of WMM, packets without QoS header will be assigned to the Best Effort queue. Please refer to the table below for mapping from 802.1p and ToS mapping to WMM:

Queue	Data Transmitted Clients to AP	IP ToS	802.1P Priority	Priority	Description
AC_BK	Background.	0x08 0x20	1, 2	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort		0, 3	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue
AC_VI	Video	0x28 0xa0	4, 5	High	Minimum delay. Time-sensitive video data is automatically sent to this queue
AC_VO	Voice	0x30 0xe0 0x88 0xb8	6, 7	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue

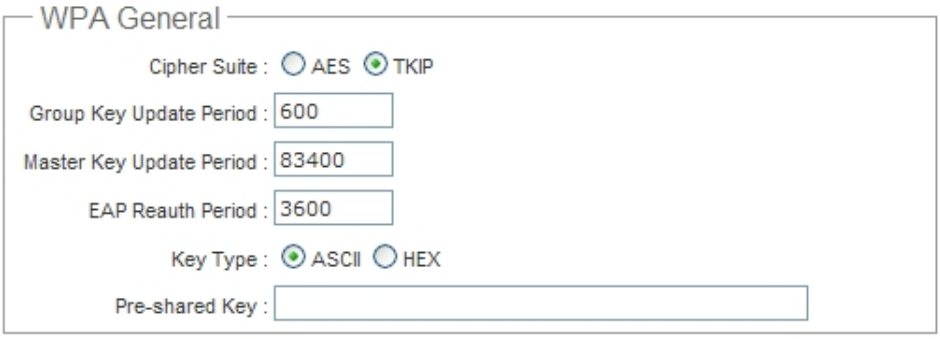
- **Maximum Clients :** The default value is **32.** You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.
- **Security Type :** Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
  - ➔ **Disable :** Data are unencrypted during transmission when this option is selected.
  - ➔ **WEP :** Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key.



  - ✓ **Key Length :** The available options are ***64 bits***, ***128 bits*** or ***152 bits***.
  - ✓ **WEP auth Method :** Enable the desired option among ***Open system*** and ***Shared***.
  - ✓ **Key Index :** key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
  - ✓ **WEP Key # :** Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters
152-bit	32 characters	16 characters

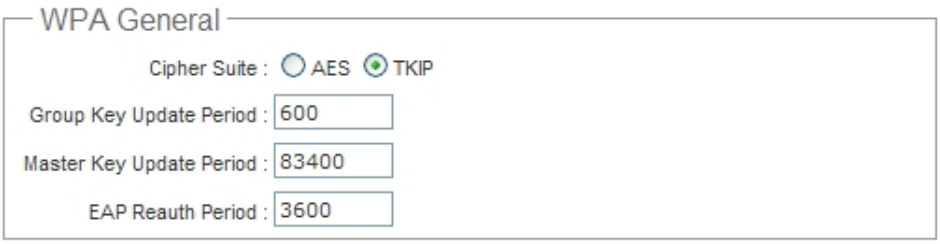
➔ **WPA-PSK/WPA2-PSK :** WPA or WPA2 Algorithms enable the system to access the network by using the WPA-PSK protected access.



- ✓ **Cipher Suite :** By default, it is TKIP. Select either AES or TKIP cipher suites
- ✓ **Group Key Update Period :** By default, it is **600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- ✓ **Master Key Update Period :** By default, it is **83400** seconds. This time interval for rekeying GMK, master key to generate GTKs, in seconds. Enter the time-length required.
- ✓ **Key Type :** Select either **ASCII** or **HEX** format for the Pre-shared Key.
- ✓ **Pre-shared Key :** Enter the pre-shared key; the format shall go with the selected key type.

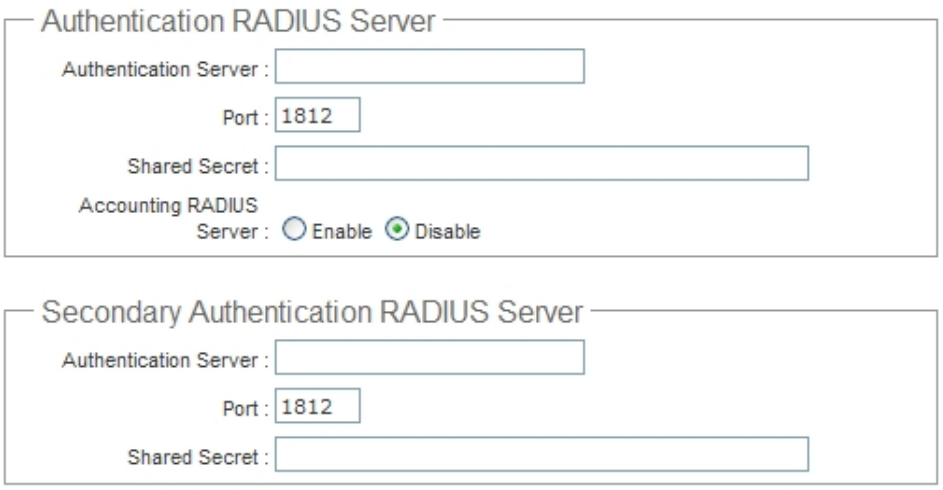
Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

➔ **WPA-Enterprise/WPA2-Enterprise:** The RADIUS authentication and encryption will apply if either one is selected.



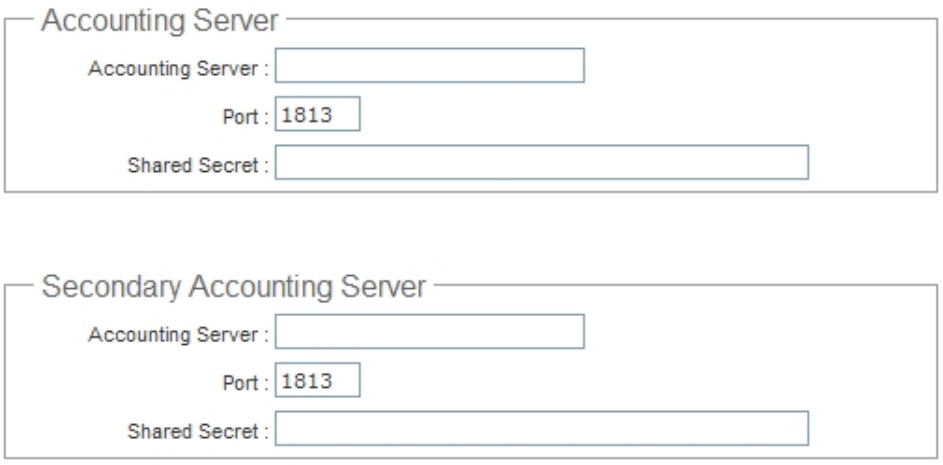
- ✓ **WPA General Settings :**
  - **Cipher Suite :** By default, it is TKIP. Select either AES or TKIP cipher suites
  - **Group Key Update Period :** By default, it's **600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
  - **Master Key Update Period :** By default, it's **83400** seconds. This time interval for rekeying GMK, master key to generate GTKs, in seconds. Enter the time-length required.
  - **EAP Reauth Period :**; By default, it's **3600** seconds; **0** second is to disable EAP Re-authentication.

✓ **Main and secondary Authentication RADIUS Server Settings :**



- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **1** to **64** characters.
- **Accounting Server :** Enable or Disable accounting features in RADIUS server.

✓ **Main or Secondary Accounting RADIUS Server Settings :**



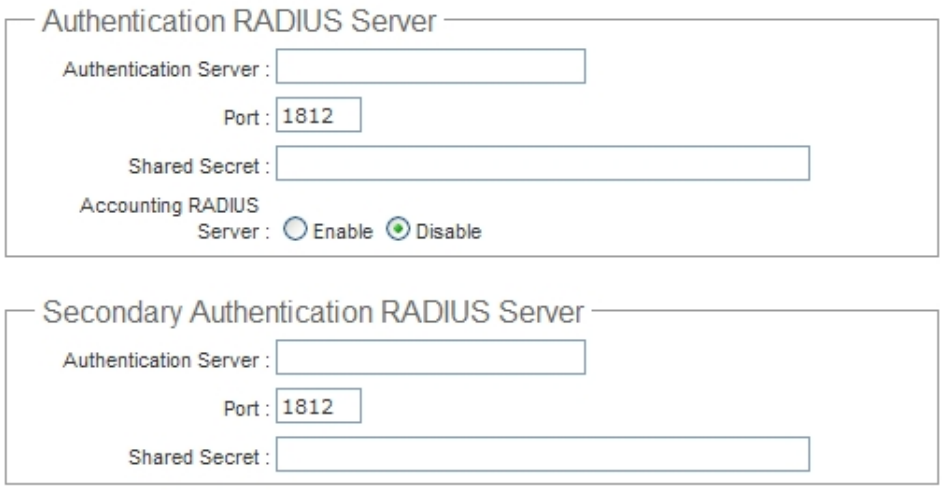
- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port : By default, it's 1813.** The port number used to communicate with RADIUS server.
- **Shared Secret :** A secret key used between system and Accounting RADIUS server. Supports **1** to **64** characters.

➔ **WEP 802.1X :** When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

✓ **Dynamic WEP Settings :**

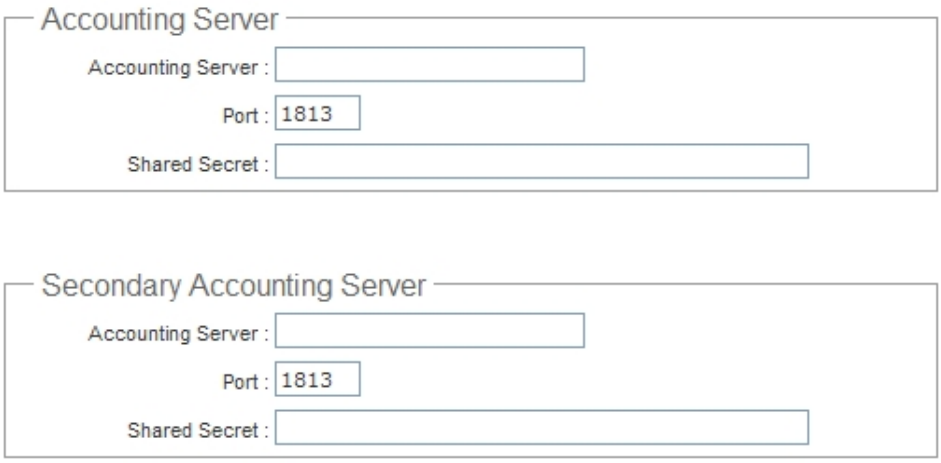
- **WEP Key length :** The available options are ***64 bits*** or ***128 bits***. The system will automatically generate WEP encryption keys.
- **WEP Key Update Period :** By default, it's 300 seconds; 0 not to rekey.
- **EAP Reauth Period :** By default, it's **3600** seconds; **0** second is to disable EAP Re-authentication.

✓ **Main and Secondary Authentication RADIUS Server Settings :**



- **Authentication Server :** Enter the IP address of the Authentication RADIUS server.
- **Port : By default, it's 1812.** The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **1** to **64** characters.
- **Accounting Server :** Enable or Disable accounting features in RADIUS server.

✓ **Main and secondary Accounting RADIUS Server Settings :**



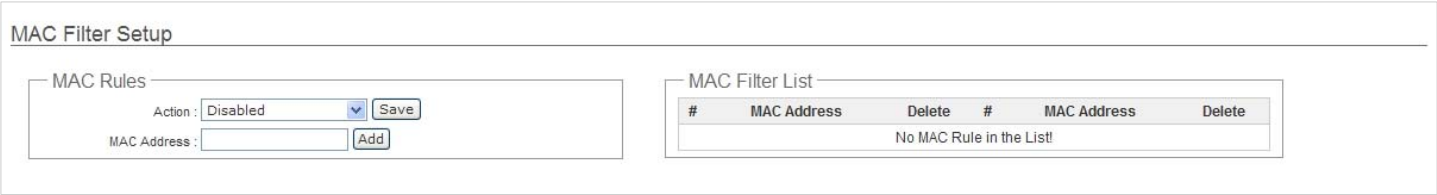
- **Accounting Server :** Enter the IP address of the Accounting RADIUS server.
- **Port : By default, it's 1813.** The port number used to communicate with RADIUS server.
- **Shared Secret :** A secret key used between system and Accounting RADIUS server. Supports **1** to **64** characters.

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

6.3.2 MAC Filter Setup

The administrator can allow or reject clients to access repeater AP.

Please click **Wireless -> MAC Filter** and follow the below settings.



- **MAC Filter Setup :** By default, it's "***Disable***". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click ***Save*** button to save your change.

  Two ways to set the MAC filter rules :

  ➔ **Only Allow List MAC**.

  The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

  ➔ **Only Deny List MAC**.

  The wireless clients in the MAC FIlter List will be **denied** to access to Access Point; All others will be allowed.

- **MAC Address :** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons**.**

Click ***Reboot*** button to activate your changes

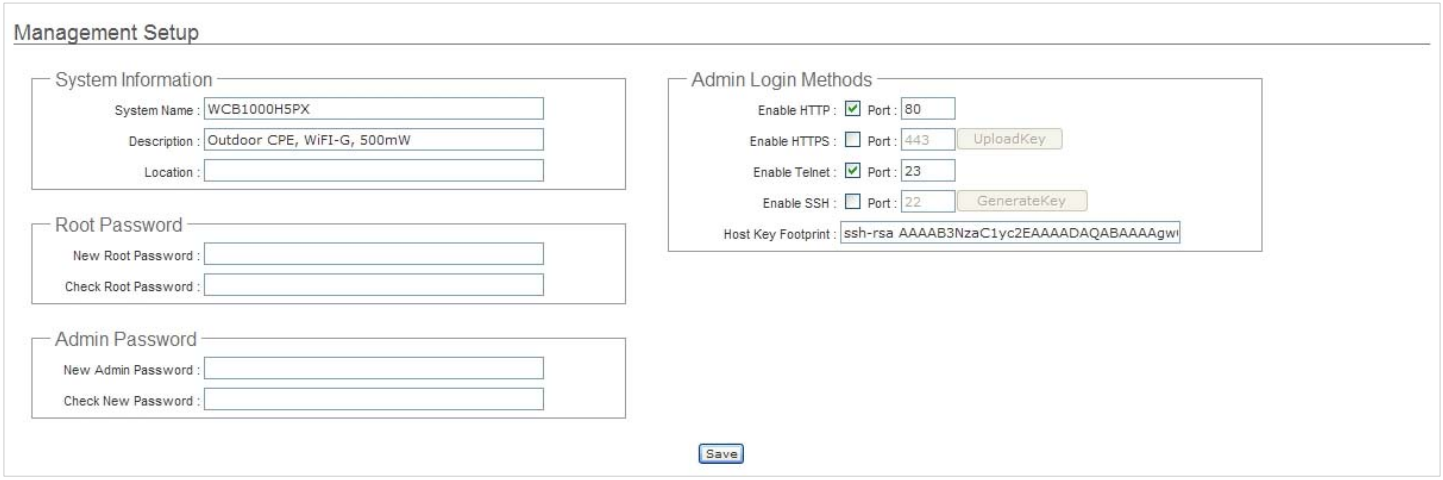
MAC Access Control is the weakest security approach. WPA or WPA2 security method is highly recommended.

6.4 System Management

6.4.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.



- **System Information**
  - ➔ **System Name :** Enter a desired name or use the default one.
  - ➔ **Description :** Provide description of the system.
  - ➔ **Location :** Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to ***Appendix C. Network manager Privileges***.

- **Root Password :** Log in as a root user and is allowed to change its own, plus admin user's password.
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Password :** Log in as a admin user and is allowed to change its own,
  - ➔ **New Password :** Enter a new password if desired
  - ➔ **Check New Password :** Enter the same new password again to check.

- **Admin Login Methods :** Only **root** user can enable or disable system login methods and change services port.
  - ➔ **Enable HTTP :** Check to select HTTP Service.
  - ➔ **HTTP Port :** The default is **80** and the range is between 1 ~ 65535.
  - ➔ **Enable HTTPS :** Check to select HTTPS Service
  - ➔ **HTTPS Port :** The default is **443** and the range is between 1 ~ 65535.

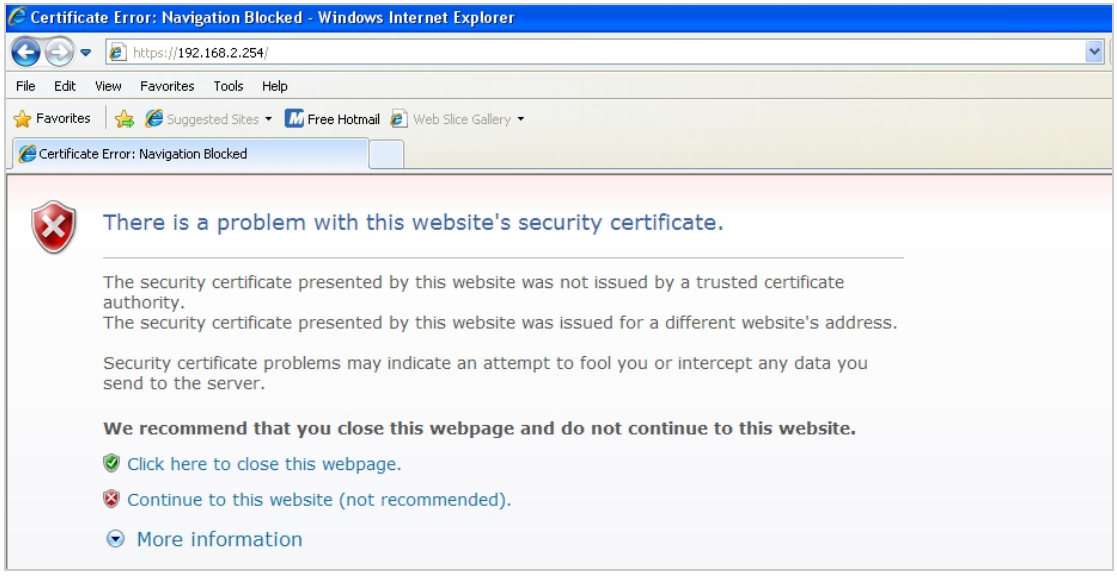
*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

  - ➔ **Enable Telnet :** Check to select Telnet Service
  - ➔ **Telnet Port :** The default is **23** and the range is between 1 ~ 65535.
  - ➔ **Enable SSH :** Check to select SSH Service
  - ➔ **SSH Port :** Please The default is **22** and the range is between 1 ~ 65535.

*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's Web GUI (https://192.168.2.254). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click "***Continue to this website***" to access the system's Web GUI. The system's Overview page will appear.

6.4.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

- **Local Time :** Display the current system time.

- **NTP Client :** To synchronize the system time with NTP server.
  - ➔ **Enable :** Check to select NTP client.
  - ➔ **Default NTP Server :** Select the NTP Server from the drop-down list.
  - ➔ **Time Zone :** Select a desired time zone from the drop-down list.
  - ➔ **Daylight saving time :** Enable or disable Daylight saving.

If the system time from NTS server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click ***Save*** button to save your changes. Click ***Reboot*** button to activate your changes

6.4.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

- **UPnP :** By default, it's "***Disable***". Select "**Enable**" or "***Disable"*** of UPnP Service.
  Click ***Save*** button to save changes and click ***Reboot*** button to activate changes

For UPnP to work in Windows XP, the "APO1000"or "APO1010" must be available in "***My Network Places***"

If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to ***Appendix D. Using UPnP on Windows XP***

6.4.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP manager and agent. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

- **SNMP v2c Enable:** Check to enable SNMP v2c.

  - ➔ **ro community :** Set a community string to authorize read-only access.
  - ➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

  SNMPv3 supports the highest level SNMP security.

  - ➔ **SNMP ro user :** Set a community string to authorize read-only access.
  - ➔ **SNMP ro password :** Set a password to authorize read-only access.
  - ➔ **SNMP rw user :** Set a community string to authorize read/write access.
  - ➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

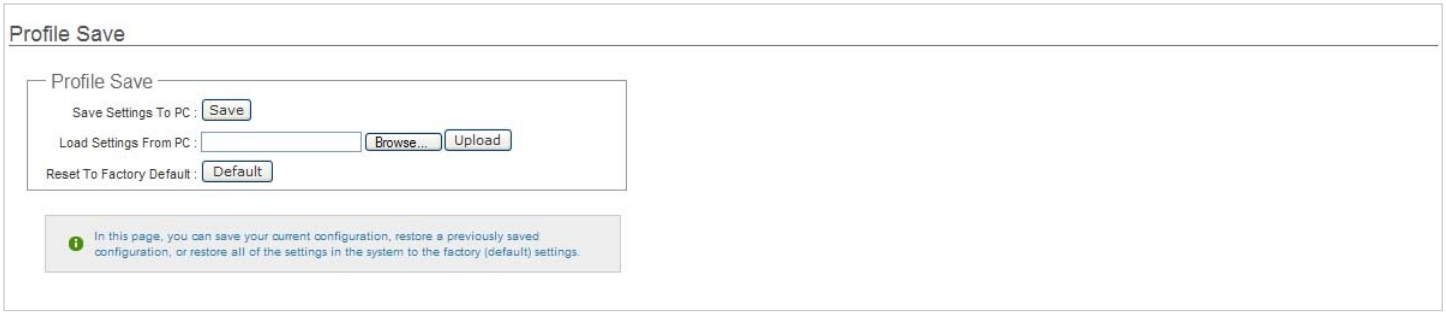
  - ➔ **Community :** Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
  - ➔ **IP :** Enter the IP addresses of the remote hosts to receive trap messages.

Click ***Save*** button to save changes and click ***Reboot*** button to activate.

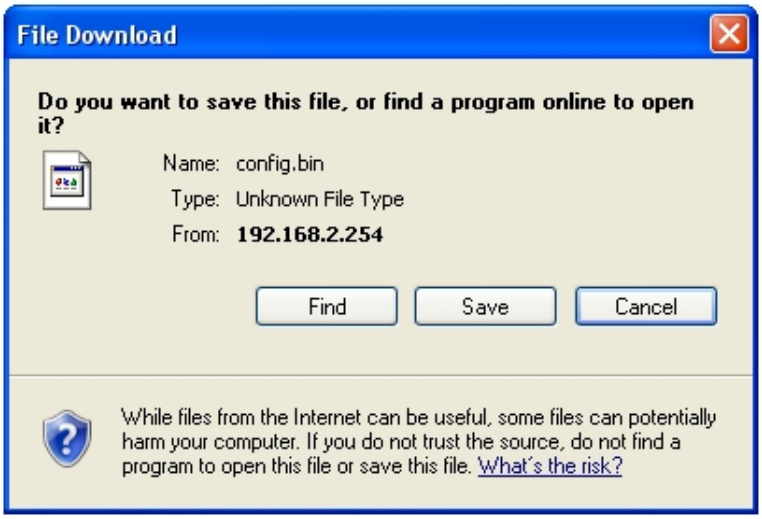
6.4.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.



- **Save Settings To PC :** Click ***Save*** button to save the current configuration to a local disk.

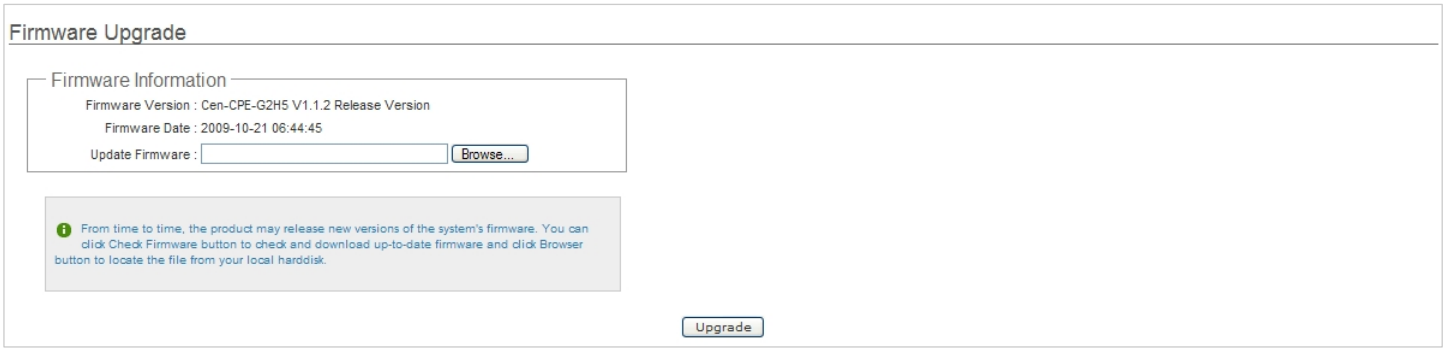


- **Load Settings from PC :** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.

- **Reset To Factory Default :** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

6.4.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **8 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click ***Browse*** button to locate the new firmware, and then click ***Upgrade*** button to upgrade.

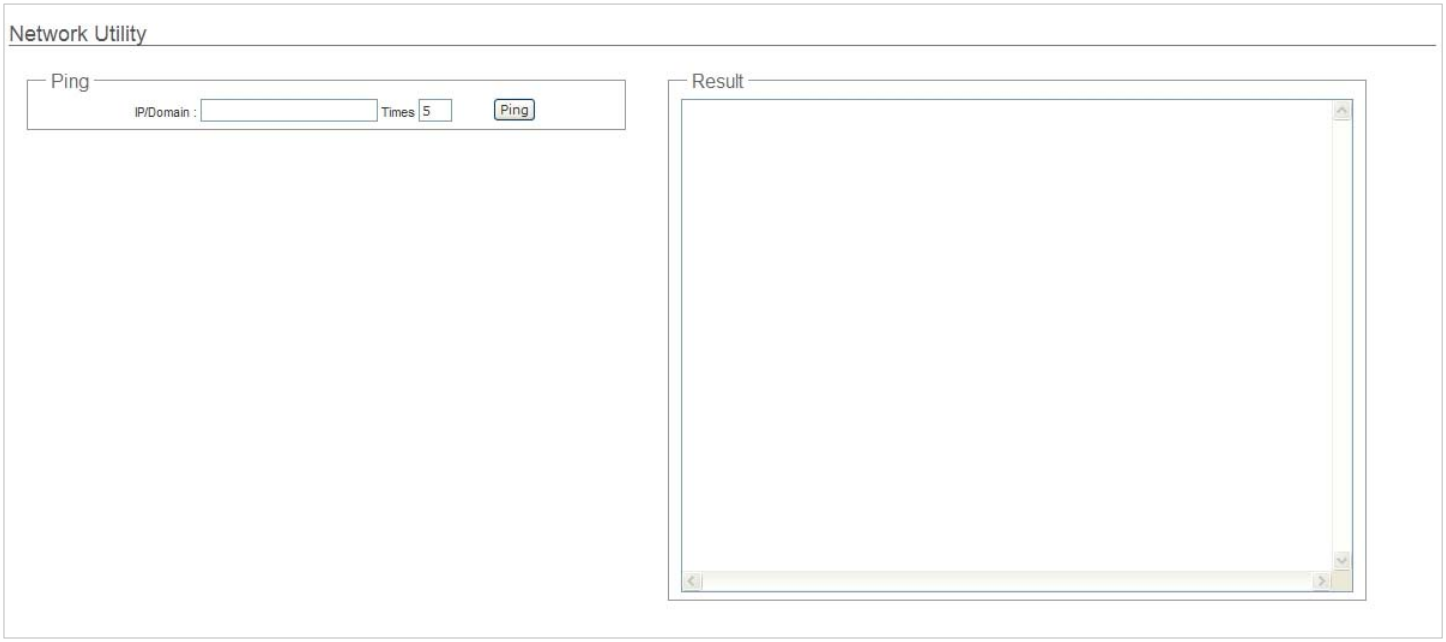


1. To prevent data loss during firmware upgrade, please back up current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.

6.4.7 Network Utility

The administrator can diagnose network connectivity via the PING utility.

Please click on **Utilities -> Network Utility** and follow the below setting.

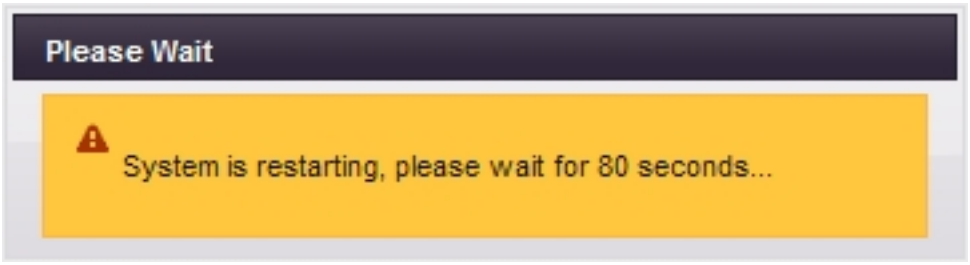


- **Ping :** This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the ***Result*** field while running the PING test.
  - ➔ **Destination IP/Domain :** Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ***ping*** button to proceed. The ping result will be shown in the **Result** field.
  - ➔ **Count :** By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

6.4.8 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click ***Reboot*** button to proceed and take around three minutes to complete.

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

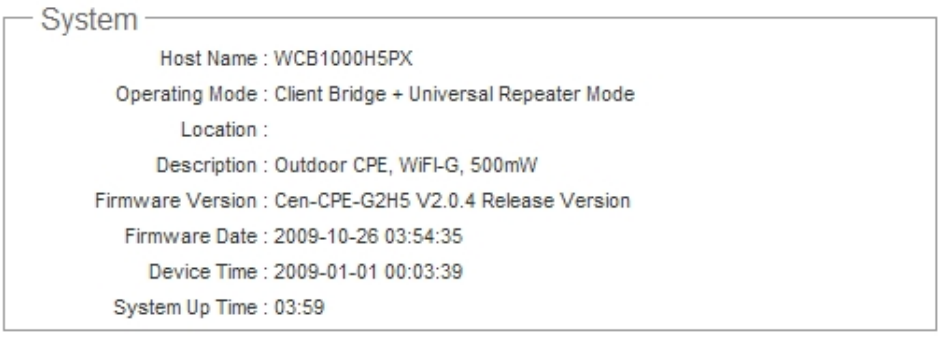
6.5 System Status

This section breaks down into subsections of ***System Overview***, ***Associated Clients Status***, ***DHCP Client List***, ***Extra Information*** and ***Event Log***.

6.5.1 System Overview

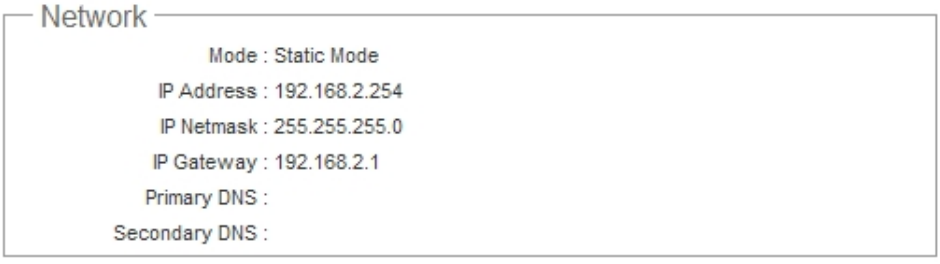
Display detailed information of ***System, Network, LAN and Wireless*** in the System Overview page.

- **System :** Display the information of the system.



  - ➔ **System Name :** The name of the system.
  - ➔ **Operating Mode :** The mode currently in service.
  - ➔ **Location :** The reminding note on the geographical location of the system.
  - ➔ **Description :** The reminding note of the system.
  - ➔ **Firmware Version :** The current firmware version installed.
  - ➔ **Firmware Date :** The build time of the firmware installed.
  - ➔ **Device Time :** The current time of the system.
  - ➔ **System Up Time :** The time period that system has been in service since last reboot.

- **Network Information :** Display the information of the Network.



  - ➔ **Mode :** Supports Static or Dynamic modes on the LAN interface.
  - ➔ **IP Address :** The management IP of system. By default, it's 192.168.2.254.

- ➔ **IP Netmask :** The network mask. By default, it's 255.255.255.0.
- ➔ **IP Gateway :** The gateway IP address and by default, it's 192.168.2.1.
- ➔ **Primary DNS :** The primary DNS server in service.
- ➔ **Secondary DNS :** The secondary DNS server in service.

- **LAN Information :** Display the detailed receive and transmit statistics of LAN interface.

- ➔ **MAC Address :** The MAC address of the LAN port.
- ➔ **Receive bytes :** The total received packets in bytes on the LAN port.
- ➔ **Receive packets :** The total received packets of the LAN port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes of the LAN port.
- ➔ **Transmit packets :** The total transmitted packets of the LAN port.

- **Wireless Station Information :** Display the information of the associated AP.

- ➔ **ESSID :** Display Extended Service Set ID of the associated AP currently.
- ➔ **Security :** Display security type of the associated AP currently.
- ➔ **Status :** Display connection status of the associated AP currently.

If the system associated with AP, the BSSID, RSSI and Last Rx Time will be show up. Below depicts the examples for associated AP of Wireless Information.

- ➔ **BSSID :** Indicate the Basic Service Set ID of the associated AP.
- ➔ **RSSI :** Indicate the RSSI of the associated AP.
- ➔ **Last Rx Time :** Indicate the last receive packet of the associated AP.
- ➔ **MAC Address :** The MAC address of the Wireless Station port.
- ➔ **Receive bytes :** The total received packets in bytes on the Wireless Station port.
- ➔ **Receive packets :** The total received packets on the Wireless Station port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes on the Wireless Station port.
- ➔ **Transmit packets :** The total transmitted packets on the Wireless Station port.

- **Wireless AP Information :** Display the detailed receive and transmit statistics of Wireless AP.

- ➔ **MAC Address :** The MAC address of the Wireless AP port.
- ➔ **Receive bytes :** The total received packets in bytes on the Wireless AP port.
- ➔ **Receive packets :** The total received packets on the Wireless AP port.
- ➔ **Transmit bytes :** The total transmitted packets in bytes on the Wireless AP port.
- ➔ **Transmit packets :** The total transmitted packets on the Wireless AP port.

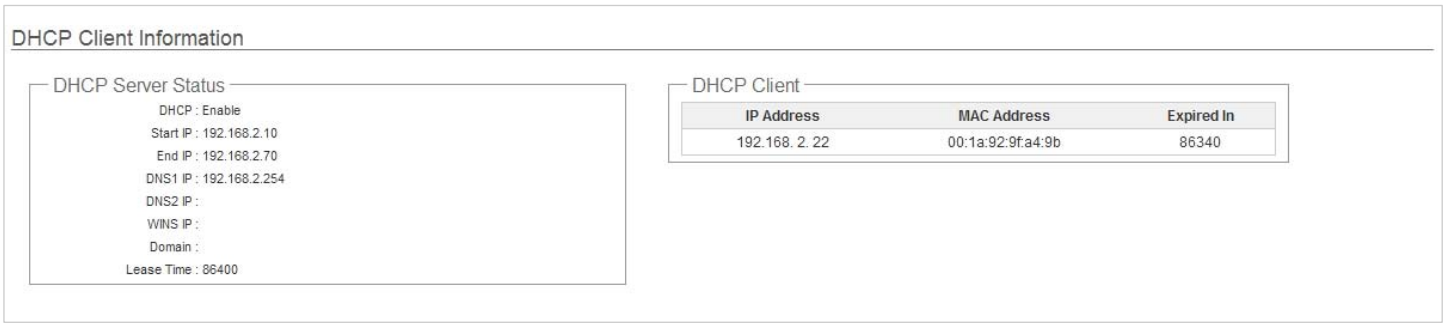
6.5.2 Associated Clients Status

It's display all associated clients on repeater AP.

- **MAC Address :** MAC address of associated clients.
- **RSSI :** RSSI of from associated clients..
- **Last TX Time :** Last inactive time period in seconds for a wireless connection.
- **Disconnect :** Click “**Delete**” button to manually disconnect a wireless client in a repeater AP.

6.5.3 DHCP Clients

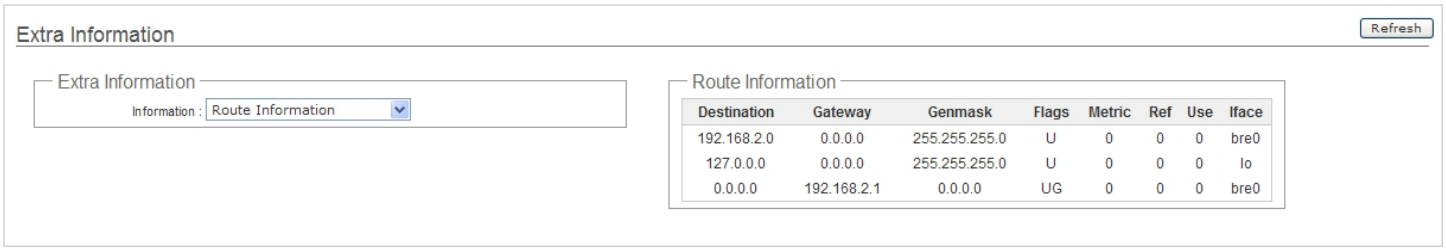
Users could retrieve DHCP server and DHCP clients' IP/MAC address via this page.



- **IP address :** IP addresses to LAN devices by DHCP server.
- **MAC address :** MAC addresses of LAN devices.
- **Expired In :** Shows how long the leased IP address will expire.

6.5.4 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.



- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

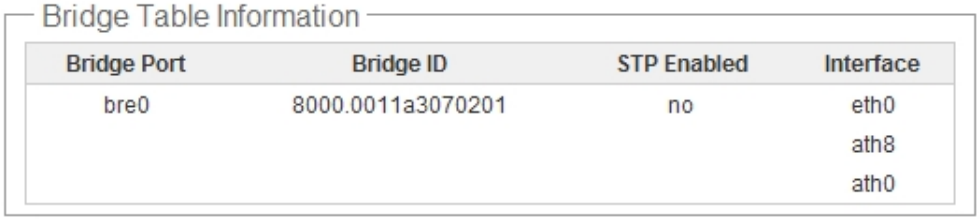
  APO1000/APO1010 could be used as a L2 or L3 device. It doesn’t support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it’s capable of being a gateway to route packets inward and outward.

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

  ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

  Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth0, ath0 and ath8).



- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

  This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.

Bridge MACs Information

Port No	MAC Address	Local	Ageing Timer
1	00:0d:0b:13:6b:16	yes	0.00
2	00:0d:0b:13:6b:18	yes	0.00
1	00:1a:92:9f:a4:9b	no	0.05

- **Bridge STP Information :** Select "**Bridge STP Information**" on the drop-down list to display a list of bridge STP information.

Bridge STP Information

bre0			
bridge id	8000.0011a3070201		
designated root	8000.0011a3070201		
root port	0	path cost	0
max age	20.00	bridge max age	20.00
hello time	2.00	bridge hello time	2.00
forward delay	15.00	bridge forward delay	15.00
ageing time	300.00	gc interval	0.00
hello timer	1.97	tcn timer	0.00
topology change timer	0.00	gc timer	11.97
flags			

eth0 (1)			
port id	8001	state	forwarding
designated root	8000.0011a3070201	path cost	100
designated bridge	8000.0011a3070201	message age timer	0.00
designated port	8001	forward delay timer	0.00
designated cost	0	hold timer	0.97
flags			

ath8 (2)			
port id	8002	state	forwarding
designated root	8000.0011a3070201	path cost	100
designated bridge	8000.0011a3070201	message age timer	0.00
designated port	8002	forward delay timer	0.00
designated cost	0	hold timer	0.97
flags			

ath0 (3)			
port id	8003	state	forwarding
designated root	8000.0011a3070201	path cost	100
designated bridge	8000.0011a3070201	message age timer	0.00
designated port	8003	forward delay timer	0.00
designated cost	0	hold timer	0.97
flags			

6.5.5 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

- **Time:** The date and time when the event occurred.
- **Facility:** It helps users to identify source of events such “System” or “User”
- **Severity:** Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message:** Description of the event.

Click ***Refresh*** button to renew the log, or click ***Clear*** button to clear all the record.

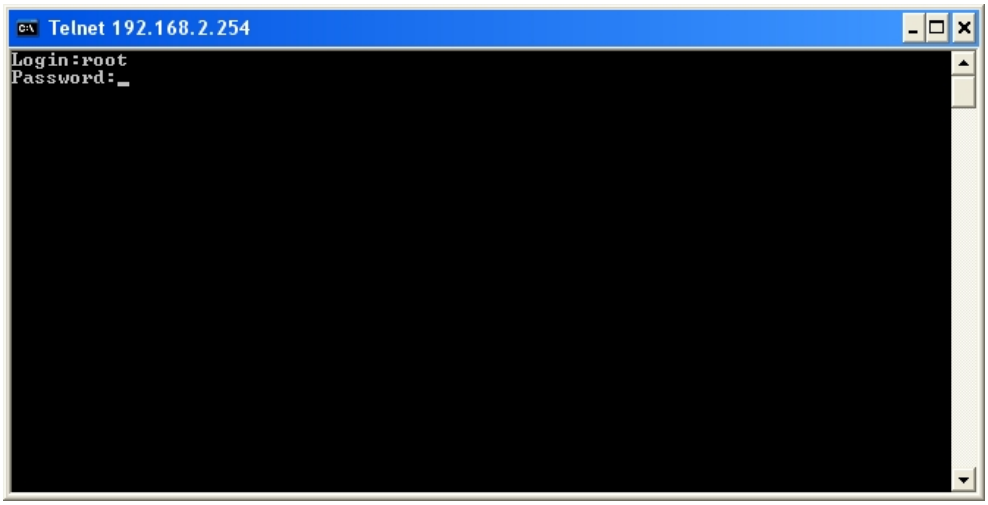
Chapter 7. Command Line Interface(CLI)

Help, **showinfo**, **pwinfo**, **set**, **reboot**, **default** and **password** functions are available via Telnet session.

7.1 Accessing the CLI with Telnet

Follow these steps to access CLI via Telnet in the Window XP:

- ➔ Click **Start -> Run**, and type "***cmd***" in the "**Run**" field. The DOS command window appears.
- ➔ Enter "***telnet 192.168.10.100***" to connect with system.

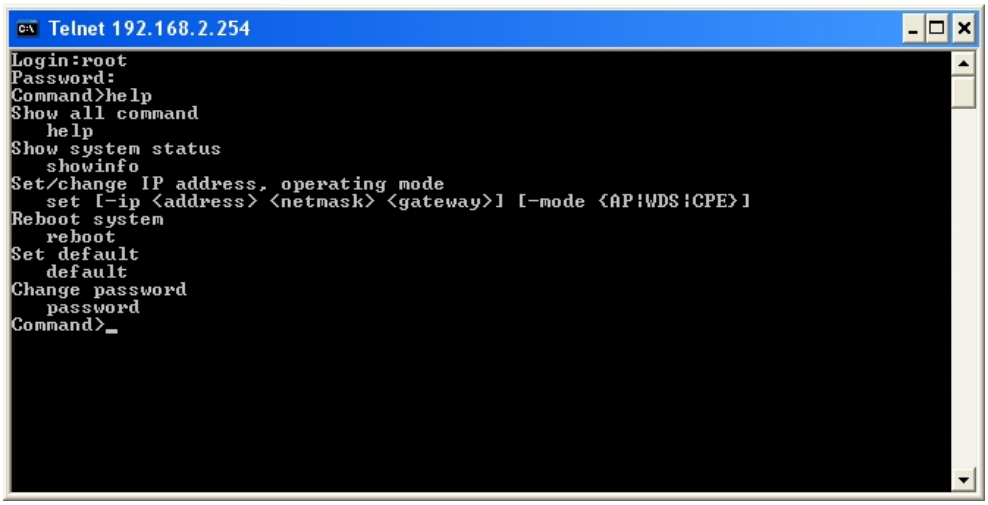


- ➔ Enter username and password, which are ***root and root*** by default, in the Telnet session,

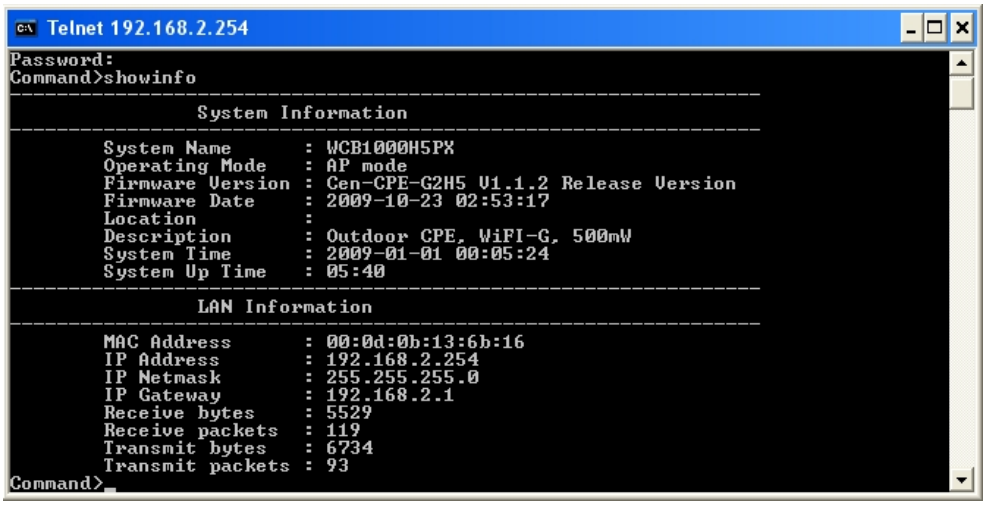
7.2 Using the CLI

After accessing the CLI, the administrator can use command on the system.

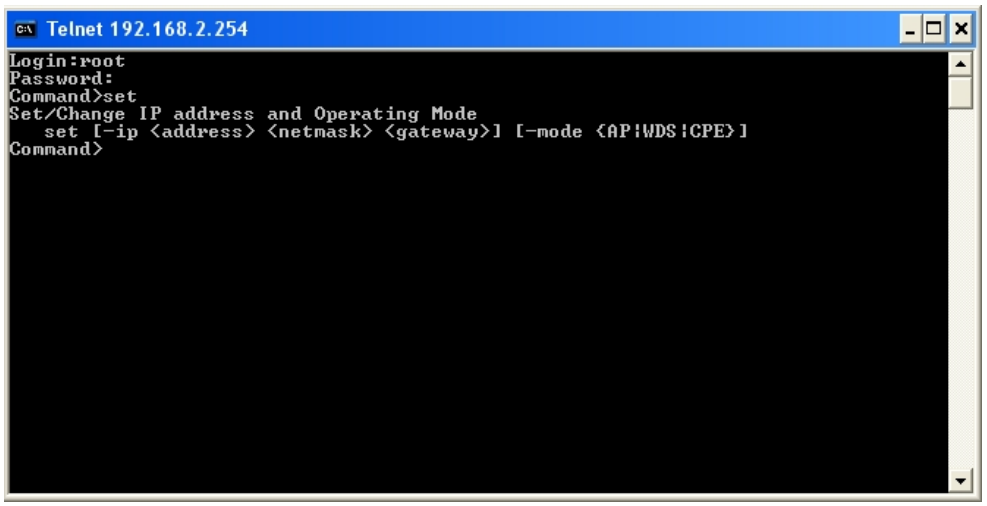
- **Using help command :** Display all commands and descriptions



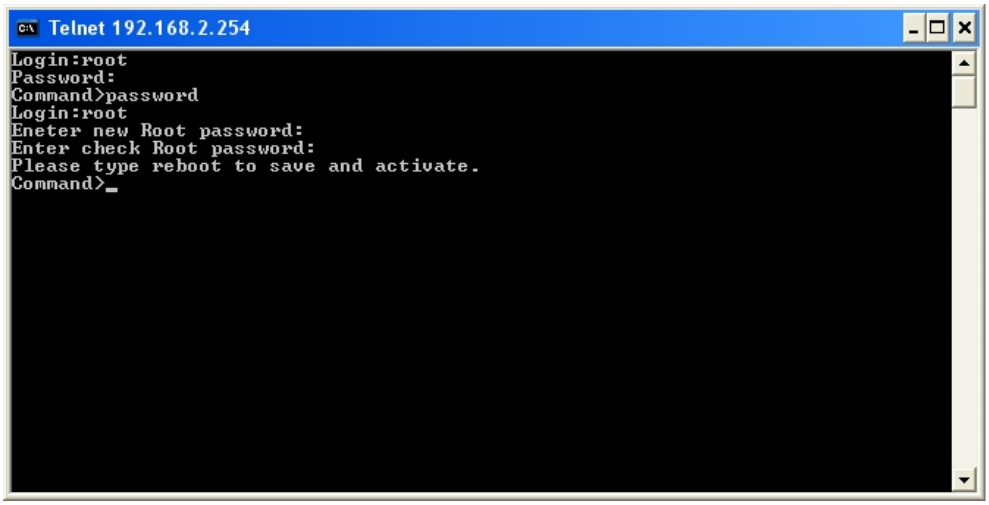
- Using **showinfo** command : Display System and LAN informations



- Using **set** command : Type **set** command to change IP address, netmask , gateway and operating mode.



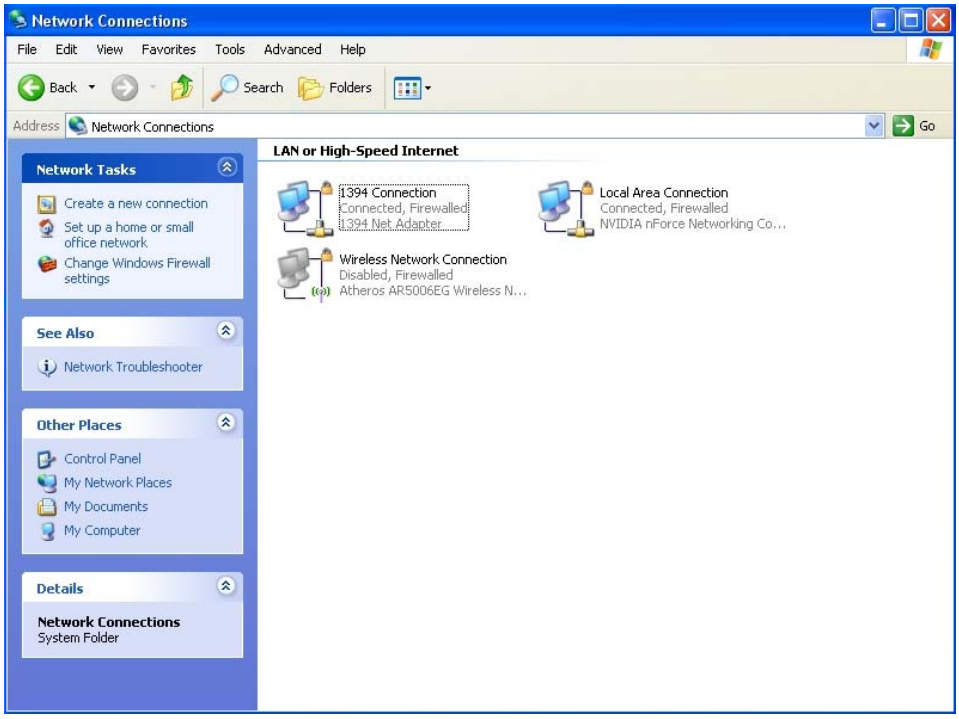
- Using **reboot** command : Restart the system
- Using **default** command : Restore system default settings
- Using **password** command : Change **root** password



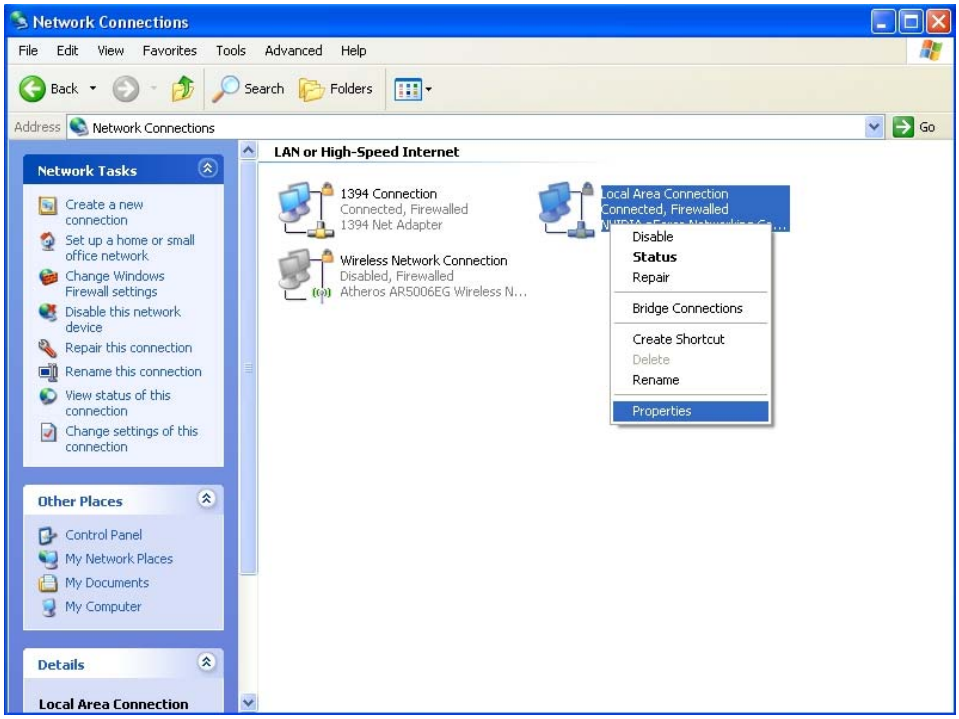
Appendix A. Windows TCP/IP Settings

▪ Windows XP

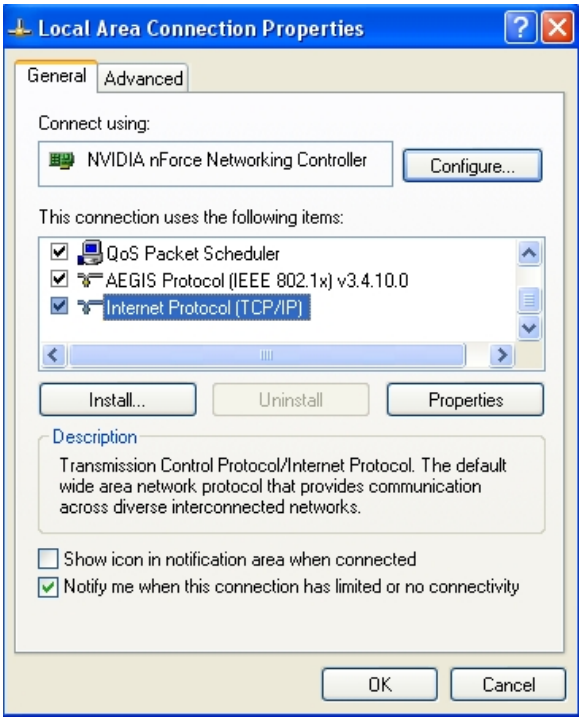
1. Click **Start -> Settings -> Control Panel**, and then "**Control Panel**" window appears. Click on "**Network Connections**", and then "**Network Connections**" window appears.



2. Click right on "**Local Area Connection**", and select ***Properties***.



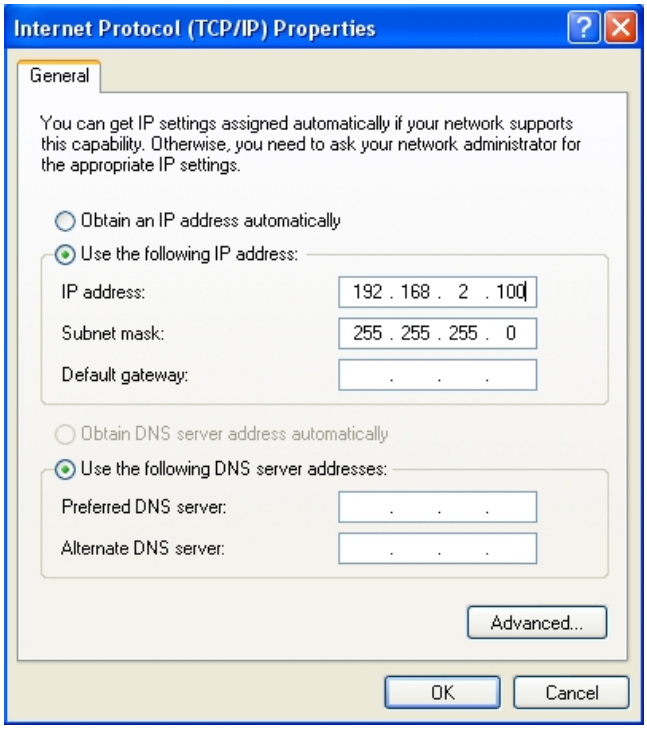
3. In “**Local Area Connection Properties**” window, select “**Internet Protocol (TCP/IP)**” and click on ***Properties*** button.



4. Select “Use the following IP address”, and type in

   IP address : 192.168.2.100

   Subnet mask : 255.255.255.0



Appendix B. WEB GUI Valid Characters

Table B WEB GUI Valid Characters

Block	Field	Valid Characters
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Primary	IP Format; 1-254
	Secondary	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
WAN	Manual MAC Address	12 HEX chars
	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.255
	IP Gateway	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
	User name	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Password	
	MTU	576 ~ 1492
	Idle Time	0 ~ 60 minutes
	Primary	IP Format; 1-254
	Secondary	IP Format; 1-254
DDNS	Hostname	Length : 32 0-9, A-Z, a-z @ - _ .
	User Name	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Password	
DHCP Server	Start IP	IP Format; 1-254
	End IP	IP Format; 1-254
	DNS1 IP / DNS2 IP	IP Format; 1-254
	WINS IP	IP Format; 1-254

	Domain	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Lease Time	600 ~ 99999999 Seconds

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Management	System Name	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Description	Length : 40 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Check New Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	HTTP Port	1 ~ 65535
	HTTPS Port	1 ~ 65535
	Telnet Port	1 ~ 65535
	SSH Port	1 ~ 65535
SNMP	RO community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO user	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RO password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =

Block	Field	Valid Characters
	RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	Community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; ` , . =
	IP	IP Format; 1-254

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
General Setup (CPE Mode)	ESSID	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	WEP Key	10, 26, 32 HEX chars
	Pre-shared Key	8 ~ 63 ASCII chars; 64 HEX chars
Advanced Setup	Slot Time	1 ~ 1489
	ACK Timeout	1 ~ 372
	CTS Timeout	1 ~ 744
	RSSI Threshold	-128 ~ 127
	Beacon Interval	1 ~ 5000
	DTIM Interval	1 ~ 15
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2346
Virtual AP Setup	ESSID	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Maximum Clients	1 ~ 32
	VLAN ID	0 ~ 4094
	WEP Key	10, 26, 32 HEX chars; 5, 13, 16 ASCII chars
	Group Key Update	10 ~ 99999999 seconds; default is 600
	Master Key Update	10 ~ 99999999 seconds; default is 83400
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Authentication Server	IP Format; 1-254
	Authentication Port	1 ~ 65535

Block	Field	Valid Characters
	Shared Secret	1 ~ 64 characters
	EAP Reauth Period	300 ~ 99999999; default is 3600, 0 is disable
	Accounting Server	IP Format; 1-254
	Accounting Port	1 ~ 65535
	WEP Key Update	0 ~ 99999999 ; default is 300, 0 is disable

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
WDS Setup	Peer's MAC Address	12 HEX chars
	VLAN ID	0 ~ 4094 ; Space is disable
	Description	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	WEP Key	10, 26, 32 HEX chars
	AES Key	32 HEX chars
IP Filter	Source Address	IP Format; 1-254
	Source Mask	0 ~ 32
	Source Port	1 ~ 65535
	Destination Address	IP Format; 1-254
	Destination Mask	0 ~ 32
	Destination Port	1 ~ 65535
MAC Filter	MAC address	MAC Format; 12 HEX chars
Virtual Server	Description	Length : 32 0-9, A-Z, a-z space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; ` , . =
	Private IP	IP Formate; 1-254
	Private Port	1 ~ 65535
	Public Port	1 ~ 65535
DMZ	IP Address	IP Format; 1-254

Appendix C. Network Manager Privileges

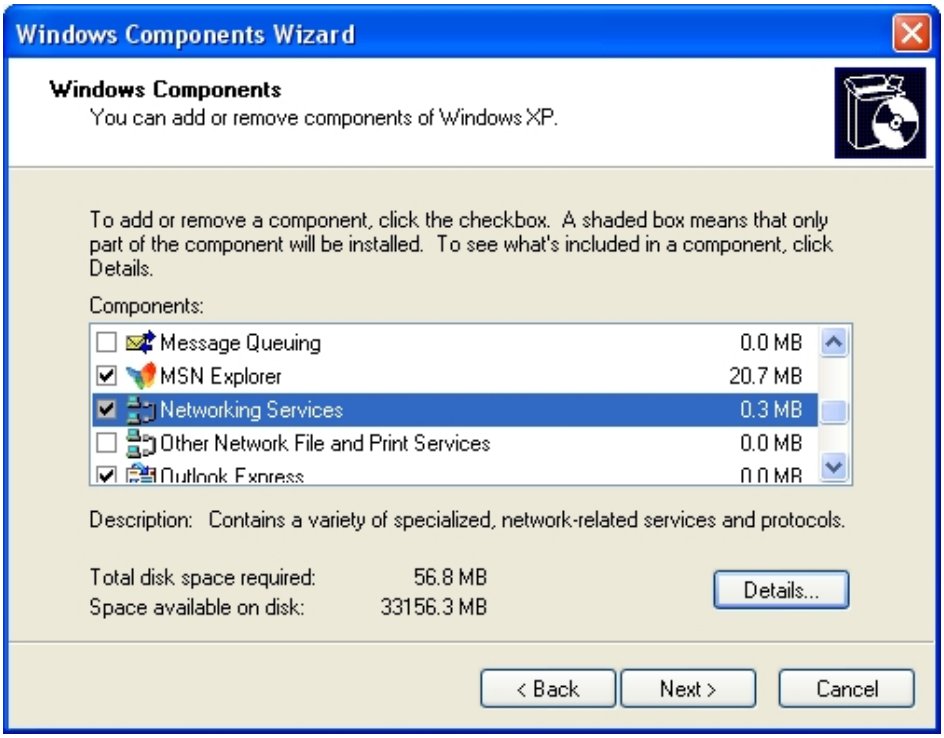
There are two system management accounts for maintaining the system; namely, the **root** and **admin** accounts are with different levels of privileges. The root manager account is empowered with full privilege to Read & Write while the admin manager account is Read only.

The following table display CPE admin account's privileges.

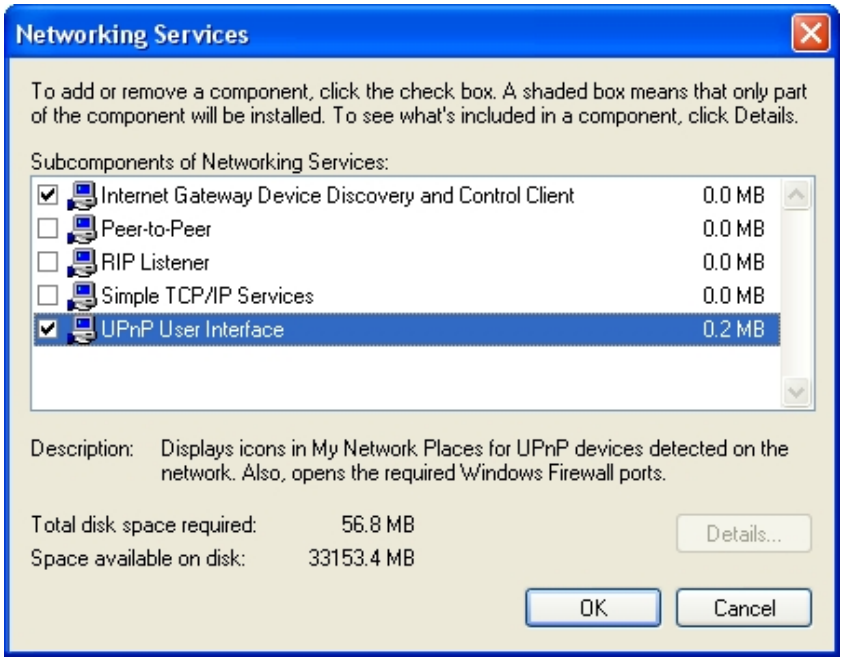
Main Menu	Sub Menu	Group	Admin Privilege
System	Operating Mode		Read
	WAN		Read
	LAN		Read & Write
	Management	System Information	Read
		Root Password	Read
		Admin Password	Read & Write
		Login Methods	Read
	DDNS		Read & Write
	Time		Read & Write
	SNMP Setup		Read
	UPNP		Read & Write
Wireless	General		Read
	Advanced		Read
	Site Survey		Read
Advance	DMZ		Read
	IP Filter		Read
	MAC Filter		Read
	Virtual Server		Read
Utilities	Profile Settings	Backup Settings	Read & Write
		Restore Settings	Read
		Reset to Default	Read
	System Upgrade		Read
	Network Utility		Read & Write
	Reboot		Read & Write

Appendix D. Enabling UPnP in Windows XP

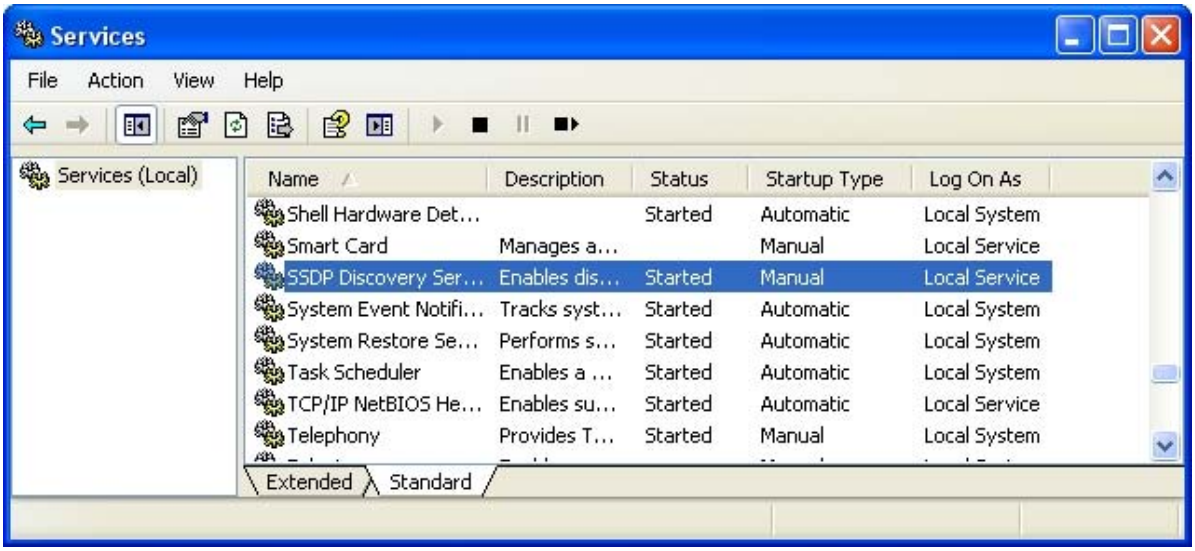
1. Open the "***Add/Remove Programs***" control panel, and then click on "***Add/Remove Windows Components***" in the sidebar. Scroll down and find "***Networking Services***", highlight it, and then click ***Details***.



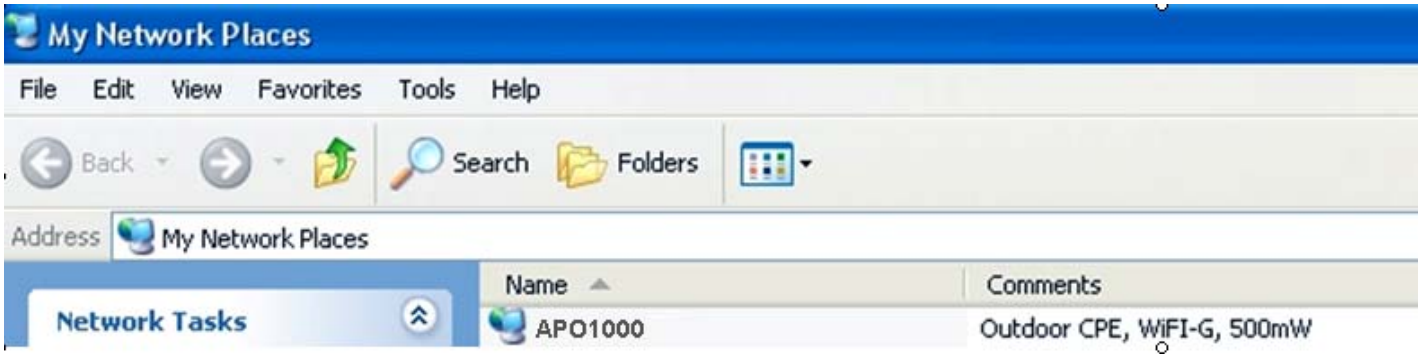
2. In the "**Networking Services**" window, ensure "***Internet Gateway Device***" and "***UPnP User Interface***" options are checked. If they are not, check to enable them, as shown below, and click Ok to continue.



3. Next, in the "**Control panel**", open the "***Administrative Tools***" and then open "***Services***". Scroll down until you find the "***SSDP Discovery Interface***". If the Status is not ***Started***, double-click on *SSDP Discovery Interface* to open the service properties. Change the startup type to ***Automatic***, then close the properties. Now, right-click on *SSDP Discovery Services*, and choose ***Start*** from the pop-up menu. The SSDP Discovery Service will then be running and start each time you boot.



4. After enabling UPnP and starting the SSDP Discovery Service, it may take few minutes for the APO1000/APO1010 to be discovered and appear in your "***My Network Places***".



Technical Support

E-mail: support@airlink101.com

Toll Free: 1-888-746-3238

Web Site: www.airlink101.com

*Theoretical maximum wireless signal rate derived from IEEE standard 802.11. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, mix of wireless products used, radio frequency interference (e.g., cordless telephones and microwaves) as well as network overhead lower actual data throughput rate. Compatibility with draft 802.11n devices from other manufactures is not guaranteed. Specifications are subject to change without notice. Photo of product may not reflect actual content.